Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
ICSC Centro Nazionale di Ricerca in HPC, Big Data and Quantum Computing

REPORT

CYBERSECURITY

OS
Osservatorio sulle tendenze e le applicazioni del Supercalcolo

Centro Nazionale di Ricerca in HPC, Big Data and Quantum Computing

Osserv-azioni su...

CYBERSECURITY

Tendenze e applicazioni del Supercalcolo, Big Data e Quantum Computing

Giugno 2025



Indice

Indice 2

Introduzione 4

Le sfide odierne nel settore cybersecurity 5

A che punto siamo in Europa? 7

A che punto siamo in Italia? 9

Dagli Osservatori Digital Innovation del Politecnico di Milano 10

AI, Supercalcolo e Big Data al servizio della cybersecurity: quali applicazioni? 13

Una piattaforma per il voto elettronico integrato sicuro: B-voting 14

Quick Shield: proteggere i documenti di nuova generazione 15

Kryptosafe: Blockchain a supporto della sicurezza dei dati 16

D-Swap: Smart Working più sicuro 17

CLEAR: una piattaforma per la sicurezza delle infrastrutture IT-OT 18

AI per la creazione di dati sintetici: la piattaforma AINDO 19

FogAtlas: un software la sicurezza dei dati nel Cloud Computing 20

SafeBot4Twin: un chatbot per la sicurezza dei dati sensibili 21

Tutelare la riservatezza dei dati sensibili nella telemedicina: Health-e-Data 22

Biosat MarketPlace: servizi satellitari on demand per la pubblica amministrazione 23

HESI: un progetto per la salvaguardia dei dati satellitari 24

Proteggere i dati aziendali dai ransomware: il progetto DCS 25

Sicurezza per le stazioni di ricarica dei veicoli elettrici: CyberGuardEV 26

SATML-B: sicurezza nelle tecniche di Machine Learning e analisi Big Data 27

ESII: un progetto per l'indagine tempestiva degli incidenti 28

WISE PACK: proteggere l'industria farmaceutica dai cyber-attacchi 29

Asset Discovery: mappare i dispositivi OT per una difesa efficace 30

Identificare le vulnerabilità nelle infrastrutture critiche: MON5 Fortezza 31

ToothPic: identità digitali non clonabili e sicurezza dei Big Data 32

Intesa Sanpaolo collabora con IBM nel testare soluzioni post quantistiche 33

Intesa Sanpaolo e IBM proteggono le transazioni digitali: la Fully Homomorphic Encryption (FHE) 34

Fortgale: sicurezza personalizzata contro i cyber threats 35

Dilaxia: servizi su misura per la protezione delle aziende 36

Le tecnologie abilitanti per la cybersecurity nel Centro Nazionale di Ricerca in HPC, Big Data e Quantum Computing 37

Il progetto CCO: il quantum computing svela le vulnerabilità della crittografia odierna 40

Migliorare la reattività agli attacchi grazie al machine learning: il progetto SCP 41

Fraud Detection: migliorare la sicurezza finanziaria grazie al quantum computing 42

Il Federated Learning come assicurazione per la privacy: il progetto FLF 43

HF: identificazione dei guasti nei sistemi HPC per prevenire vulnerabilità 44

Megatrend e segnali deboli collegati alle sfide nella cybersecurity 45

Armi cibernetiche e information warfare: nuovi pericoli 45

La cybersicurezza e le tecnologie quantum: la nascita della crittografia post-quantistica 46

La cybersicurezza nelle Smart Cities: protezione dei dati e non solo 48

Crowdsourced Cyberattacks: un pericolo che amplia i confini geografici di un conflitto 49

Bibliografia 50

Introduzione

Il settore della cybersecurity sta attualmente subendo numerose innovazioni in svariati ambiti: nelle tecnologie applicate, nella governance e nell'impianto normativo.

L'utilizzo sempre più pervasivo dei dispositivi IoTs crea un network di sensori e apparecchi che scambiano continuamente dati di ogni tipo, inoltre la crescente disponibilità di applicazioni di intelligenza artificiale, soprattutto AI generativa (GenAI), rende più facile la buona riuscita di cyber-attacchi e furti di dati. Tra le principali minacce cyber si possono annoverare:

- Phishing/spear phising: un attaccante invia una mail credibile ai dipendenti di un'organizzazione per carpire informazioni confidenziali
- Data breach: un furto di dati, i quali possono essere distrutti o rivenduti sul deep web
- Distributed Denial of Services (DDoS): un attaccante infetta con un malware i server di un determinato servizio, impedendo agli utenti di accedervi e di erogare normalmente le loro funzioni
- Ransomware: un furto di dati o un DDoS finalizzato alla richiesta di riscatto

Le nuove tecnologie non sono solo però uno strumento in mano agli attaccanti, ma hanno numerose implicazioni positive nell'evoluzione della cybersecurity.

In questo report analizziamo le misure e le iniziative prese in Europa e poi in Italia.

Presentiamo poi degli *use case* che mostrano progetti di innovazioni in diversi contesti aziendali e istituzionali italiani, che integrino soluzioni basate su intelligenza artificiale, supercomputing e quantum computing nel settore della cybersecurity.

La seconda metà del report si concentra sui progetti della Fondazione ICSC dedicati alla cybersecurity.

Infine, mostriamo trend e scenari futuri, che delineano le prospettive a lungo termine, evidenziando i principali sviluppi tecnologici, economici e normativi attesi.



Eleonora Barelli
Eleonora.barelli@ifabfoundation.org



Eleonora Ocello
Eleonora.ocello@ifabfoundation.org



Ethel Gallo
Ethel.gallo@ifabfoundation.org



Giada Sechi
Giada.sechi@studio.unibo.it

Le sfide odierne nel settore cybersecurity

Con il termine cybersecurity si intendono tutte le attività legate alla prevenzione, individuazione, mitigazione e risposta alle minacce informatiche; il concetto di sicurezza informatica è quindi in continua evoluzione, al pari con l'innovazione tecnologica e l'evoluzione stessa delle minacce cyber.

Tra le principali autorità in materia di cybersecurity si riscontra l'Agenzia dell'UE per la cybersecurity (ENISA), che tra i suoi compiti annovera appunto la mappatura delle sfide emergenti la definizione delle priorità in merito alle nuove tecnologie con potenziali implicazioni per la cybersicurezza.

Ad esempio, il rapido sviluppo e la maggiore disponibilità delle tecnologie AI le ha portate ad essere sempre più integrate in diversi settori, dalla sanità e finanza ai veicoli autonomi e ai servizi al cliente e, sebbene queste tecnologie apportino indubbi benefici, possono anche aprire nuovi scenari di manipolazione e metodi di attacco, oltre a generare nuove sfide in materia di sicurezza e privacy.

È quindi fondamentale riconoscere il doppio ruolo dell'AI nella sicurezza informatica: se da un lato può essere sfruttata per manipolare i risultati attesi, dall'altro può potenziare le operazioni di cybersicurezza e contribuire a mitigare gli attacchi avversari. In aggiunta, l'uso dell'IA come strumento per la cybersicurezza rende essenziale lo sviluppo di misure specifiche che garantiscano l'affidabilità e la sicurezza degli stessi sistemi o strumenti basati su AI.

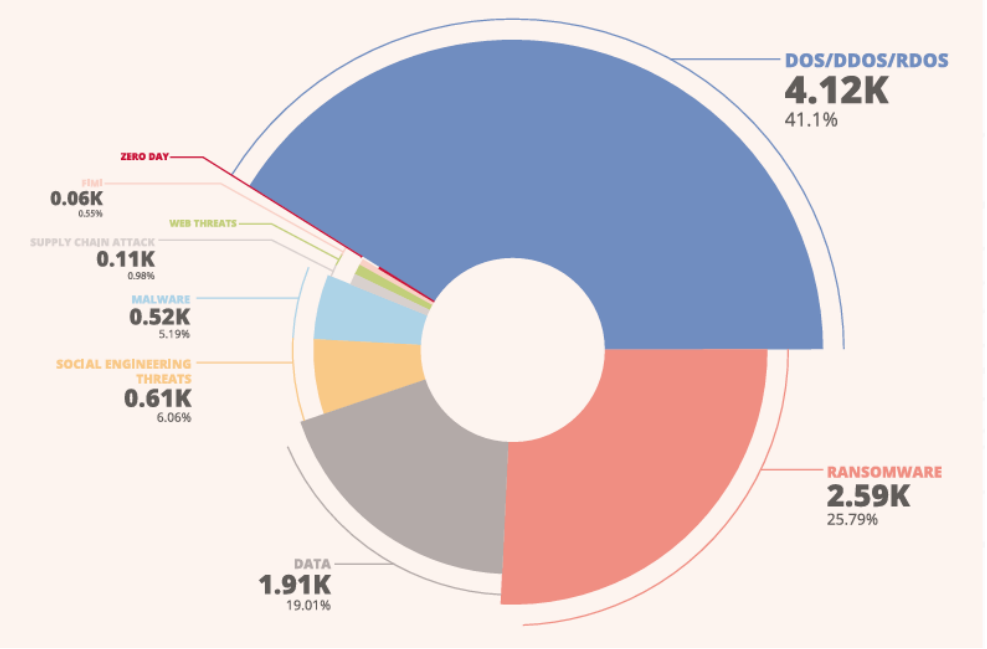


Figura 1: Minacce cyber divise per tipologia di attacco (Credits: 2024 Report on the State of the Cybersecurity in the Union - https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union)

Anche le applicazioni di quantum computing hanno una funzione ambivalente, specialmente nell'ambito della crittografia, componente fondamentale della cybersicurezza. L'introduzione della tecnologia quantistica promette infatti importanti avanzamenti in diversi settori, ma rappresenta anche una sfida rilevante per le infrastrutture di sicurezza: il calcolo quantistico solleva infatti preoccupazioni in merito all'integrità e alla sicurezza delle soluzioni crittografiche

attualmente in uso, portando allo sviluppo del campo della crittografia post-quantistica, con l'obiettivo di creare soluzioni crittografiche progettate per resistere alle minacce potenziali derivanti dai computer quantistici.

Per quanto riguarda invece i principali bersagli dei cyber attacchi all'interno dell'UE, come si può osservare nella Figura 2, le pubbliche amministrazioni si posizionano al primo posto, seguite dal settore dei trasporti e da quello finanziario. L'attenzione dei cyber criminali è quindi principalmente rivolta verso le PA, le quali comprendo strutture ospedaliere, scuole, tribunali e amministrazioni locali e nazionali, poiché queste, nella società odierna sempre più interconnessa, gestiscono servizi vitali e raccolgono grandi quantità di dati. Sono infatti sempre di più le città e le aree urbane che si dotano di dispositivi smart e soluzioni IoTs, prendendo così il nome di Smart Cities, e rendendo sempre più servizi come trasporti, sanità locale, sicurezza stradale e amministrazione, interconnessi e digitali, di conseguenza producendo, analizzando e immagazzinando un enorme volume di dati, che si prefigurano come l'obiettivo perfetto per i cyber criminali.

È quindi fondamentale che, per la sicurezza digitale e fisica di tutti i cittadini, vengano spese misure di cybersecurity in questo ambito. Le minacce cyber non hanno infatti impatti solo sulla privacy dei singoli e delle istituzioni, ma hanno anche forti impatti economici, sociali e nei casi più gravi anche di sicurezza fisica delle comunità coinvolte.

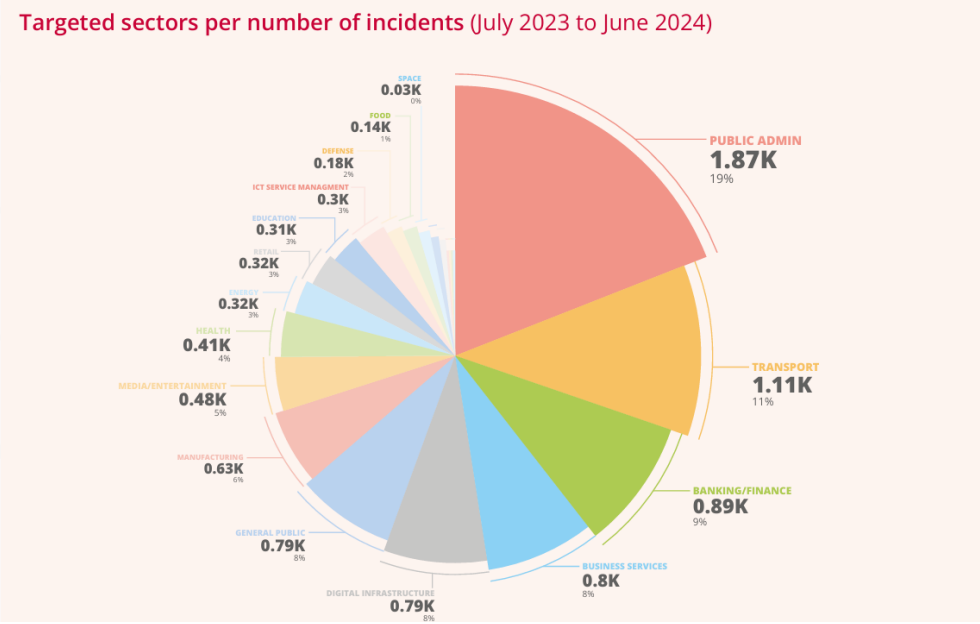


Figura 2: Settori target degli attacchi cyber (Credits: 2024 Report on the State of the Cybersecurity in the Union - https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union)

A che punto siamo in Europa?

L'Unione Europea è consapevole della trasformazione digitale in corso in svariati ambiti della società e dei rischi correlati, pertanto ha attuato numerose iniziative finalizzate all'evoluzione del concetto e delle applicazioni di cybersecurity.

Nel 2020 la Commissione Europea ha annunciato la *Nuova Strategia Europea per la Cybersicurezza* per garantire resilienza e sovranità tecnologica, aumentando la capacità operativa dell'UE di prevenire e rispondere ai cyber-attacchi e promuovendo inoltre la cooperazione fra Stati e la creazione di un cyberspazio globale e aperto.

Dal punto di vista legislativo la più grande innovazione promossa dall'UE è stata la direttiva NIS2, entrata in vigore nel gennaio 2023 e a cui tutti gli stati membri si devono conformare per aumentare il livello comune di cybersecurity all'interno dell'UE. Questa direttiva va quindi a colmare le carenze delle norme precedenti relative alla NIS1 e amplia il loro campo di applicazione a nuovi settori in base al grado di interconnessione e alla loro importanza per l'economia e per la società, introducendo obblighi stringenti di gestione del rischio e di segnalazione degli incidenti per le aziende. Le aziende si distinguono in due categorie: i soggetti essenziali, come i fornitori di energia, il settore dei trasporti, banche e servizi finanziari, aziende ospedaliere e farmaceutiche, e i soggetti importanti, come servizi di smaltimento dei rifiuti e servizi postali.

La direttiva NIS2 mira quindi a promuovere una cultura della cybersicurezza, invitando gli stati membri ad una collaborazione più stretta attraverso organismi come il Computer Security Incident Response Teams (CSIRT), l'Agenzia UE per la cybersicurezza (ENISA) e EU-CyCLONe, l'organismo dedicato alla gestione delle crisi su vasta scala.

Per quanto riguarda le risposte e la prevenzione ai cyber-attacchi, la NIS2 non cita esplicitamente l'impiego dell'intelligenza artificiale, ma fa comunque riferimento a tecniche che ne implicano l'impiego, come la gestione proattiva dei rischi, le analisi predittive per l'anticipazione degli attacchi, l'automazione delle notifiche e delle risposte agli incidenti ed infine la scansione proattiva delle vulnerabilità.

A completamento del quadro proposto dalla NIS2 nel dicembre 2024 è entrato in vigore il Cyber Resilience Act che introduce requisiti obbligatori di cybersecurity per i prodotti software e hardware durante tutto il loro ciclo di vita, migliorando così la resilienza a tutte le minacce cyber dei dispositivi presenti sul mercato europeo. I produttori devono quindi conformarsi a nuovi obblighi di sicurezza di progettazione rimanendo continuamente aggiornati e adottando procedure di valutazione della conformità per assicurare che i loro prodotti rispettino i requisiti.

Inoltre, i sistemi di intelligenza artificiale classificati come ad alto rischio devono rispettare requisiti specifici per la protezione dei dati e la gestione dei rischi, come la robustezza e l'affidabilità. L'AI è anche però enfatizzata come strumento di sicurezza contro minacce come gli attacchi di avvelenamento dei dati e gli attacchi antagonistici, rispecchiando il crescente ruolo dell'IA nella difesa informatica.

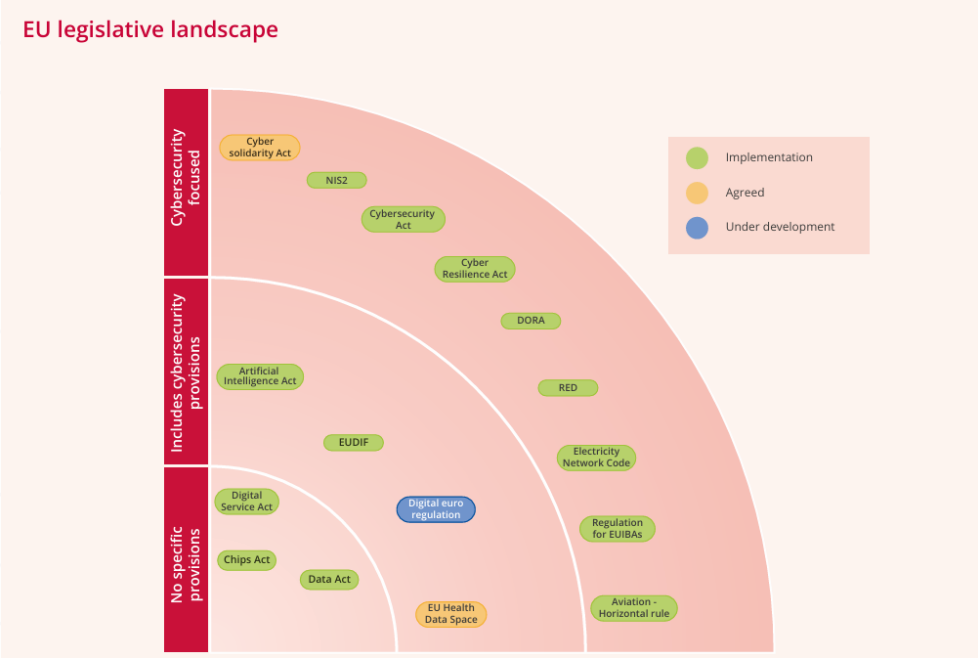


Figura 3: Panormana legislativo europeo in ambito cybersecurity (Credits: 2024 Report on the State of the Cybersecurity in the Union - https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union)

Il principale organo dell'UE dedicato all'implementazione della cybersicurezza è ENISA, istituita nel 2004 e potenziata dal Cybersecurity Act, agenzia che ha lo scopo di uniformare il livello di cybersicurezza all'interno dell'Unione, migliorando l'affidabilità dei prodotti, dei servizi e dei processi ICT attraverso schemi di certificazione. L'agenzia supporta lo sviluppo e l'implementazione delle varie policies dell'Ue collaborando con gli Stati membri, a cui fornisce assistenza tecnica, e con gli altri organismi sovranazionali europei. Attraverso la condivisione delle conoscenze, lo sviluppo delle capacità e la sensibilizzazione, l'Agenzia inoltre lavora per rafforzare la fiducia nell'economia connessa, aumentare la resilienza delle infrastrutture dell'Unione e mantenere la società e i cittadini europei digitalmente sicuri.

EU-CyCLONe è invece una rete di cooperazione per le autorità nazionali degli Stati membri responsabili della gestione delle crisi cibernetiche. La rete è stata formalizzata nel gennaio 2023, con l'entrata in vigore dell'articolo 16 della NIS2 e ha come principale obiettivo quello di sviluppare una cooperazione efficace tra stati membri e organi UE, necessaria per rispondere a incidenti cibernetici, attacchi e crisi di grande portata.

Tra le principali attività di EU-CyCLONe si riscontrano quindi: il supporto alla gestione coordinata di incidenti e crisi, l'incentivazione di uno scambio regolare di informazioni rilevanti tra gli Stati membri e le istituzioni, la valutazione delle conseguenze degli incidenti, proponendo possibili misure di mitigazione, il supporto al processo decisionale in relazione alle crisi, in alcuni casi anche discutendo i piani nazionali di risposta a incidenti cibernetici su larga scala.

Dal punto di vista organizzativo EU-CycCLONe si colloca all'interno di ENISA, la quale funge da Segretario della rete e fornisce tutte le infrastrutture, gli strumenti e il supporto necessari per la prevenzione e la risposta agli attacchi. Perdipiù la Commissione Europea può essere inclusa come membro attivo nei casi in cui un incidente cibernetico di grande portata possa avere un impatto significativo su servizi e attività dell'UE.

A che punto siamo in Italia?

In Italia il principale ente di riferimento è L'Agenzia per la Cybersicurezza Nazionale (ACN), istituita nel 2021 e competente per quanto riguarda la tutela degli interessi nazionali nell'ambito cibernetico. Tra le varie occupazioni, ACN si occupa di prevenire e mitigare i cyber-attacchi in territorio nazionale e si muove per l'attuazione della *Strategia Nazionale di Cybersicurezza*, da ultimarsi entro il 2026.

La *Strategia nazionale di cybersicurezza 2022-26* mira a rendere l'Italia più sicura e resiliente al fronte delle nuove sfide poste dall'incessante sviluppo tecnologico e dalla trasformazione digitale. La Strategia identifica tre obiettivi fondamentali: la protezione degli asset strategici basata su un approccio orientato alla gestione del rischio, grazie ad un quadro normativo coerente e l'applicazione di controlli sicurezza; la risposta a minacce di natura cyber attraverso l'impiego delle capacità nazionali e l'attivazione delle procedure di allertamento di tutti gli attori dell'ecosistema nazionale; infine lo sviluppo consapevole di tecnologie digitali, il sostegno alla ricerca e il rafforzamento della competitività industriale.

Nell'ambito della Missione 4 del Piano Nazionale di Ripresa Resilienza (PNRR) è stato istituito anche il partenariato esteso dedicato alla cybersecurity: SERICS – Security and Rights in CyberSpace che coordina università, aziende, enti di ricerca e pubbliche amministrazioni per la realizzazione di progetti in ambito Cyber, articolandosi in 10 Spoke che ricoprono diversi ambiti e applicazioni della sicurezza informatica.

Tra le iniziative italiane si riscontra anche CyberSec, la conferenza internazionale promossa dal giornale Cybersecurity Italia che nel 2025 è arrivata alla sua quarta edizione, incentrata sulle nuove tecnologie che stanno rivoluzionando la sicurezza informatica e conseguentemente intitolata "AI, Crittografia Post-Quantum, Spionaggio e Geopolitica: il nuovo mondo della Cybersecurity". L'edizione del precedente indagava invece l'evoluzione tecnologica della cybersicurezza nell'era dell'AI, segno che anche sul panorama nazionale le rapide evoluzioni delle minacce cyber dovute all'impiego dell'AI, delle tecnologie HPC e del quanto computing sono state recepite e vengono comprese nella loro pericolosità, andando a spronare lo sviluppo di soluzioni di difesa che a loro volta integrino queste tecnologie, in modo da sopperire preventivamente ad eventuali vulnerabilità e garantire una risposta rapida ed efficace a tutte le crisi di tipo cyber.

A questo proposito, l'ACN è uno dei principali finanziatori del progetto IT4LIA AI Factory, una delle prime piattaforme strategiche di intelligenza artificiale che sfrutterà la potenza di calcolo di un supercomputer all'avanguardia, progettato per l'AI e con sede presso il Tecnopolo di Bologna. L'avvio di questo progetto promuoverà l'adozione di soluzioni AI in settori chiave, prima fra tutti la cybersecurity e attraverso un modello organizzativo *one-stop-shop*: l'AI Factory semplificherà l'accesso a dati di grande valore e a una vasta gamma di servizi, incentivando la collaborazione tra ricercatori, sviluppatori, startup e PMI. L'ACN mira infatti a sfruttare le potenzialità dell'AI Factory per l'impiego dell'intelligenza artificiale come strumento difensivo verso gli attacchi sempre più frequenti verso infrastrutture critiche nazional

Dagli Osservatori Digital Innovation del Politecnico di Milano

L'Osservatorio Cybersecurity & Data Protection ha prodotto il report "Artificial intelligence e cybersecurity: gli impatti per la società e per le organizzazioni" basato su una ricerca del 2023 che mette in luce il rapporto bivalente tra AI e cybersecurity: una stessa applicazione di intelligenza artificiale può infatti rivelarsi un importante strumento di protezione, sia un'arma efficacie per sferrare attacchi dannosi.

La maggiore diffusione e accessibilità dell'applicazioni AI, in particolare di quelle generative, ha rafforzato le capacità offensive dei cybercriminali, che impiegano questo strumento principalmente in due modalità: o potenziando le classiche tecniche di attacco come ransomware, DDoS e phishing, rendendole più efficaci ed estendendo l'entità dei danni inflitti, oppure andando a creare un livello di disinformazione tale da mettere a repentaglio la riservatezza e la disponibilità delle informazioni, utilizzando tecniche di manipolazione come i deepfake.

Come si può osservare dalla Figura 4, le grandi organizzazioni italiane sono consapevoli delle gravità delle minacce cyber potenziate dall'AI, mettendo al primo posto in termini di preoccupazione le campagne di social engineering, ovvero i fenomeni di phishing e spear phishing, rese più efficaci e personalizzate.

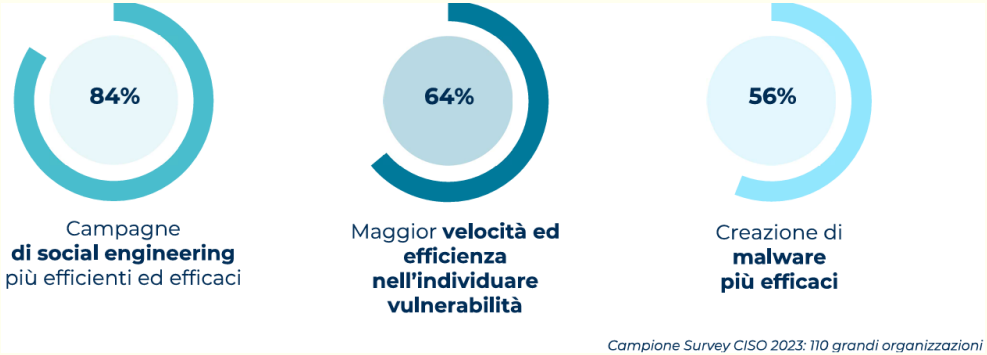


Figura 4: La percezione delle organizzazioni dell'utilizzo malevolo dell'AI: tecniche di attacco (Credits: Osservatorio Cybersecurity & Data Protection 2023 - Politecnico di Milano - www.osservatori.net)

Come si evidenzia nel report "Lo scenario della cybersecurity in Italia nel 2024" dell'Osservatorio Cybersecurity & Data Protection, i rischi in termini di sicurezza e protezione dei dati subentrano anche quando sono le stesse aziende a fare uso di applicativi AI: le capacità autonome dell'intelligenza artificiale possono infatti generare decisioni o azioni non intenzionali, che possono avere un impatto negativo sull'immagine dell'azienda. Inoltre, i modelli AI, come i GPT aziendali, possono rappresentare un punto di accesso a banche dati e informazioni sensibili per eventuali cyber-attaccanti. Consapevoli di queste vulnerabilità, nel 2024 la quasi totalità delle grandi aziende si è dotata di un presidio sulla cybersecurity, nella si può infatti osservare nella Figura 5 come l'82% delle grandi organizzazioni abbia attivato un processo di gestione del rischio cyber, integrandolo all'interno dei processi di risk management aziendali, o considerandolo come un rischio a se stante.



Figura 5: La gestione del rischio cyber nelle grandi organizzazioni italiane (Credits: Osservatorio Cybersecurity & Data Protection 2024 - Politecnico di Milano - www.osservatori.net)

In aggiunta, nel 2024 solo il 4% delle grandi organizzazioni intervistate non possedeva al suo interno un team dedicato alla cybersecurity, tuttavia le imprese faticano ad inserire nuovi esperti e tendono ad interfacciarsi sempre più frequentemente con partner esterni: in particolare, la maggior parte delle grande aziende mantiene internamente la definizione della strategia di cybersecurity e l'analisi dei rischi, implementando invece tramite outsourcing attività più onerose come le Security Operations e l'identificazione e il rilevamento delle minacce.

Anche per via di queste dinamiche di esternalizzazione, la cybersecurity si è confermata nel 2024 la principale priorità di investimento in innovazione digitale per il quarto anno consecutivo, con una crescita del 15% del mercato italiano di sicurezza informatica. Questa spinta nel mercato italiano è stata principalmente causata dall'aumento degli investimenti nei servizi da parte delle grandi organizzazioni, investimenti che per la prima volta hanno superato la quota per le soluzioni tecnologiche. Questa crescente spesa in servizi è guidata sia dall'aumento dei servizi gestiti, che permetto l'esternalizzazione delle attività operative, sia dall'aumento dei servizi professionali, che offrono competenze specializzate per migliorare la gestione del rischio cyber.

Per quanto riguarda le quote di spesa suddivise per aree di sicurezza nella Figura 6 viene evidenziato come la maggior parte degli investimenti confluisca ad aumentare la sicurezza delle infrastrutture e dei network, mentre ricevono una minima parte della spesa le componenti di Cloud Security e IoT/OT security.

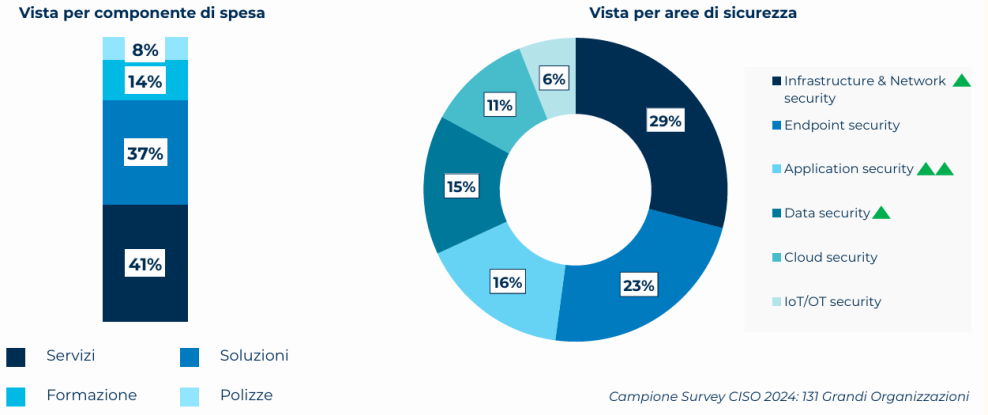


Figura 6: La ripartizione degli investimenti in ambito cyber nelle grandi organizzazioni italiane (Credits: Osservatorio Cybersecurity & Data Protection 2024 - Politecnico di Milano - www.osservatori.net)

Il 2024 ha visto anche una veloce evoluzione degli strumenti tecnologici che ha portato il consolidamento di soluzioni di cybersecurity all'interno delle grandi organizzazioni.

Siccome una delle principali e più efficaci modalità di attacco si configura nel social engineering, l'interesse delle grandi aziende è principalmente volta alla mitigazione del rischio legato al fattore umano, investendo in soluzioni anti-spam, anti-phishing, in sistemi di gestione delle credenziali, di autenticazione multi-fattore e di autenticazione biometrica. Per quanto riguarda la salvaguardia dei dati aziendali, le aziende stanno investendo principalmente in soluzioni di Data Loss Prevenzioni (DLP), mentre stanno guadagnando popolarità le soluzioni SOAR (security Orchestrati on, Automation and Response) che permettono di rispondere in maniera immediata e automatizzata agli incidenti cyber, coordinando in modo efficiente le azioni di difesa.

La Generative AI (GenAI) può rappresentare un ulteriore sviluppo nelle tecniche della cybersecurity grazie alla sua capacità di interagire grazie a tecniche avanzate di Natural Language Processing (NLP): il machine learning e l'AI permettono infatti alti livelli di automazione, che abbinate con la semplificazione dell'interazione con i sistemi di sicurezza di GenAI, permetto un miglioramento dell'efficienza operativa e della fruibilità dei tool. L'intelligenza artificiale generativa consente inoltre l'automazione delle policy di cybersecurity, adattandole dinamicamente alle normative in evoluzione e garantendo la conformità con gli standard regolatori. La Figura 7 mostra la diffusione delle soluzioni AI e GenAI nelle grandi organizzazioni.

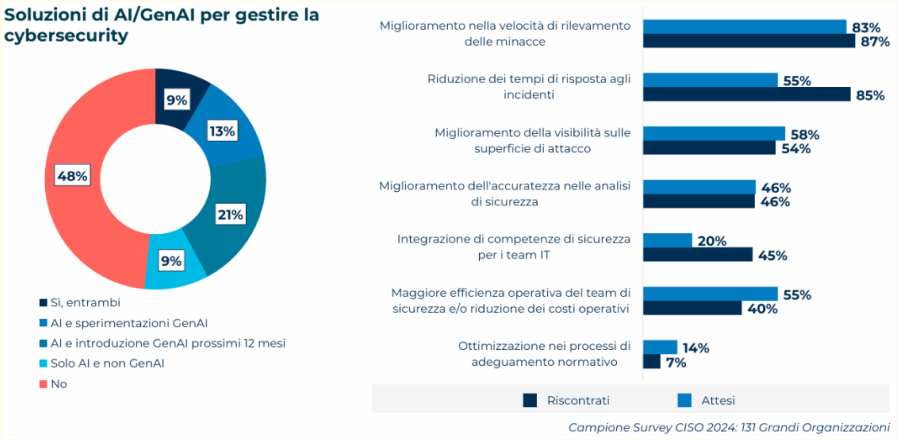


Figura 7: Soluzioni di AI GenAI nelle grandi organizzazioni italiane (Credits: Osservatorio Cybersecurity & Data Protection 2024 - Politecnico di Milano - www.osservatori.net)

I benefici derivati dall'adozione di AI e GenAI si manifestano in maniera molto eterogenea, con impatti significativi su più fronti: il risultato più evidente appare nel miglioramento della velocità di rilevamento delle minacce cyber, seguito dalla riduzione dei tempi di risposta agli incidenti.

Nel 2024 si è inoltre verificata innovazione legislativa in materia di cybersecurity con l'entrata in vigore della direttiva NIS2, che mira all'elevazione del livello di resilienza comune ai cyber-attacchi, aggiornando i requisiti di sicurezza delle organizzazioni definite come essenziali o importanti. Attualmente, il 62% delle grandi organizzazioni ha avviato il processo di adeguamento della NIS2, mentre il 30% no si riconosce all'interno del perimetro regolamentare, il restante 8% non ha intrapreso alcune azioni per comprendere gli impatti di questa direttiva.

AI, Supercalcolo e Big Data al servizio della cybersecurity: quali applicazioni?

La strategie di cybersecurity spaziano ambiti vari e diversi fra loro: l'individuazione delle vulnerabilità, la prevenzione delle minacce, la creazione di una governance e risk management efficienti, l'implementazione delle risposte ai cyber attacchi, la compliance alle direttive sovranazionali in materia e la formazione ai dipendenti.

Con riferimento a tutti questi ambiti, molte aziende, enti, istituti di ricerca e università, anche dietro la spinta delle nuove normative europee, hanno deciso di utilizzare le più accurate tecnologie e strumenti digitali per creare piattaforme, startup o progetti per metterli a servizio dei policy makers, dei ricercatori, del settore dell'industria o anche dell'intera comunità con il fine ultimo di aumentare il livello comune di cybersecurity e resilienza agli attacchi informatici.

Abbiamo mappato alcuni esempi virtuosi di realtà, piccole e grandi, che utilizzano le nuove tecnologie (Big Data, Supercalcolo, Intelligenza Artificiale) nell'ambito della cybersecurity.

Nei paragrafi seguenti, presentiamo alcuni casi d'uso, evidenziando:

- abstract del progetto;
- benefici attesi e/o obiettivi del progetto;
- tecnologia utilizzata nel progetto.

Per condividere nuovi casi d'uso, si può compilare il form al seguente link: https://forms.office.com/e/6ZNCp04rUW .

Una piattaforma per il voto elettronico integrato sicuro: B-voting

L'impiego del voto elettronico è una prospettiva reale e comune in svariati paesi del mondo: Net Service ha per questo motivo creato B-voting, una piattaforma che supera gli attuali limiti dei tradizionali sistemi di e-voting, sollevando l'ente organizzatore della votazione dalla responsabilità di garantire l'anonimato e la non alterabilità del voto, trasferendo l'onere di tali garanzie alla piattaforma Blockchain.

B-Voting garantisce tutti i requisiti essenziali richiesti a un sistema di voto digitale, soprattutto in caso di voto elettivo, garantendo un voto non tracciabile e non alterabile, mantenendo la verificabilità del conteggio dei voti. La piattaforma assicura inoltre maggiore trasparenza rispetto al voto tradizionale, consentendo di controllare l'esito della transazione di voto in qualsiasi momento, permettendo flessibilità e configurabilità, così che il cliente possa personalizzare il proprio modello di votazione. La sicurezza della piattaforma è garantita sia dal suo impianto di privacy-by-design, sia dalla sua natura volta alla disintermediazione e alla tracciabilità di tutte le transazioni.

B-voting ha quindi come componente centrale l'impiego della tecnologia Blockchain, sfruttata sia per l'esecuzione che la memorizzazione delle operazioni, inoltre questa tecnologia per sua natura non richiede importanti interventi di manutenzione, garantendo un risparmio sui costi di gestione. In sintesi, il processo di voto si basa su una chiave univoca realizzata tramite QR-code che permette all'utente di creare un account sulla Blockchain, su questo account l'elettore riceverà poi la notifica di apertura delle votazioni e potrà esprimere la sua preferenza. La cifratura della lista prescelta avviene con la chiave pubblica dell'Ente e successiva scrittura sulla Blockchain del voto cifrato. Durante lo scrutinio verranno poi decifrate, con la chiave privata della votazione, le informazioni cifrate e infine verrà fatta la scrittura in chiaro del voto sullo smart contract di scrutinio. Ogni votante, tramite lo smart contract di scrutinio, potrà in aggiunta invocarne i metodi per conoscere in tempo reale le operazioni di scrutinio.

netservice
Empowering Digital Evolution
Home | L'eccellenza italiana nel settore IT | Net Service | Net Service S.p.A.

Quick Shield: proteggere i documenti di nuova generazione

Il progetto Quick Shield nasce per rispondere alla crescente esposizione delle PA e imprese italiane ed europee ad attacchi informatici sempre più sofisticati. In linea con le direttive europee NIS2 e con i paradigmi GDPR, la piattaforma integra tecnologie post-quantum per cifratura e firma digitale, storage distribuito e condiviso tra diverse organizzazioni, motorizzazione dei contenuti su blockchain e strumenti di Intelligenza Artificiale on-premise, fornendo un ecosistema resiliente, tracciabile e con una struttura di privacy-by-design.

Quick Shield si pone l'obiettivo di rafforzare la sicurezza informatica di Pubbliche Amministrazioni e Imprese attraverso una piattaforma DMS evoluta per la protezione dei contenuti digitali da attacchi informatici sempre più sofisticati. Il progetto integra tecnologie di cifratura e storage distribuito per garantire continuità operativa anche in caso di compromissione di intere infrastrutture CED. A ciò si affiancano strumenti di intelligenza artificiale, progettati per operare esclusivamente all'interno del perimetro organizzativo, in grado di supportare l'utente nell'individuazione di anomalie e nella gestione sicura dei propri documenti digitali.

Per raggiungere questi obiettivi, Quick Shield combina attività di ricerca e sviluppo finalizzate allo studio e all'adozione di nuove tecnologie di cifratura post-quantum, con l'integrazione di soluzioni consolidate di storage distribuito, blockchain e intelligenza artificiale, facilmente interoperabili anche su infrastrutture esistenti. Il progetto adotta un approccio modulare e scalabile che consente alle organizzazioni di mettere in sicurezza i propri contenuti digitali attraverso strumenti avanzati di protezione e automazione, mantenendo il pieno controllo sui dati all'interno del perimetro organizzativo e riducendo al minimo la dipendenza da fornitori esterni.

netservice
Empowering Digital Evolution
Home | L'eccellenza italiana nel settore IT | Net Service | Net Service S.p.A.

Kryptosafe: Blockchain a supporto della sicurezza dei dati

La salvaguardia dei dati sensibili in tutte le fasi della loro vita, come la raccolta, l'analisi e lo storing, è uno dei principali obiettivi delle strategie di cybersecurity, al fine di prevenire e limitare le conseguenze malevole di un attacco di tipo Data Breach. Net Service, grazie al fondo europeo di Sviluppo regionale e in collaborazione con la regione Puglia, sta sviluppando la piattaforma Kryptosafe, finalizzata proprio all'archiviazione sicura dei dati personali.

L'obiettivo principale della piattaforma Kryptosafe, basata sulla tecnologia Blockchain, è la realizzazione di soluzioni totalmente sicure da fornire agli enti che si trovano a gestire dati personali o sensibili di terzi in outsourcing, senza che questo faccia diminuire la loro efficienza o renda più difficile la gestione del loro core business, evitando loro di perdere investimenti precedenti.

Il progetto Kryptosafe prevede interventi di ricerca industriale tesi a studiare e definire un prototipo di piattaforma che, basata sulla tecnologia Blockchain, consentirà di fornire una soluzione totalmente sicura con rischio quasi zero, si procederà poi con interventi di sviluppo sperimentale per testare il prototipo della piattaforma in un ambiente rilevante e realizzandone una versione per il mercato estero.

netservice
Empowering Digital Evolution
Home | L'eccellenza italiana nel settore IT | Net Service | Net Service S.p.A.

D-Swap: Smart Working più sicuro

Lo Smart Working è sempre di più diffuso all'interno delle organizzazioni, comportando un'esponenziale crescita nelle esigenze di collaborazione, monitoraggio e condivisione del lavoro, favorendo un interscambio di dati, documenti e informazioni. D-Swap è una piattaforma integrata, ideata da Net Service, che coniuga le esigenze operative tipiche dello Smart Working con le necessità relative alla sicurezza delle informazioni gestite e scambiate.

La soluzione può portare benefici a tutte le aziende pubbliche e private che necessitano di una garanzia totale su quanto scambiato nell'ambito della piattaforma, in particolar modo quando tali informazioni possono assumere rilevanza da un punto di vista della riservatezza, sia del dato, sia dei partecipanti e delle relative comunicazioni. D-Swap adotta infatti un approccio di security-by-design, si basa su un'infrastruttura stabile, matura e open source, favorendo un approccio distribuito e decentralizzato, rispettando gli standard di sicurezza e riservatezza grazie alla crittografia End-to-End e alla sua impostazione GDPR compliant.

L'affidabilità e l'interoperabilità del sistema Cloud è garantita da svariati protocolli, come il protocollo di comunicazione Matrix Open Standard, il protocollo Open Source IPFS per la gestione dei file e la crittografia End-to-End. D-Swap consente inoltre di gestire e attuare diverse azioni tutte sulla stessa piattaforma grazie alla sua divisione in quattro aree funzionali: la Business Chat, la Video e Audio conference, La gestione File e le Notifiche Intelligenti, un altro aspetto innovativo si riscontra inoltre nella possibilità di configurare il grado di privacy di chat, file condivisi e call da parte degli utenti.

netservice
Empowering Digital Evolution
Home | L'eccellenza italiana nel settore IT | Net Service | Net Service S.p.A.

CLEAR: una piattaforma per la sicurezza delle infrastrutture IT-OT

Net Service, nel contesto dello Spoke 8 della Fondazione SERICS "Security and Rights in the Cyberspace", svilupperà il progetto CLEAR - Cybersecurity Laboratory for EdgeComputing and Advanced Research che consisterà nella realizzazione di un avanzato laboratorio di cybersecurity, finalizzato alla validazione dei risultati teorici e allo sviluppo di Proof of Concept e framework utili per l'esecuzione di esperimenti.

L'obiettivo di CLEAR è quello di erigersi a punto di riferimento per la ricerca e lo sviluppo di soluzioni innovative nella protezione delle infrastrutture IT-OT, in un contesto globale in cui la crescente digitalizzazione rende le infrastrutture critiche e i servizi essenziali vulnerabili alle minacce informatiche in continua evoluzione, rendendo necessario un approccio alla gestione del rischio cibernetico.

Per il raggiungimento dei suoi obiettivi, il progetto CLEAR provvederà alla creazione di un'infrastruttura avanzata capace di raccogliere Big Data da ambienti IT-OT, analizzando metriche e integrando i dati in un DataLake progettato con un approccio privacy-by-design e by-default, in conformità con il GDPR e le normative europee di settore. L'innovatività del progetto si riscontra anche nell'utilizzo di tecniche Federated Learning ed Edge Computing per lo sviluppo un sistema capace di garantire scalabilità, sicurezza e adattabilità in tempo reale. L'architettura decentralizzata basata su Edge Computing minimizza inoltre i punti singoli di errore e garantisce la continuità operativa anche in caso di attacchi, in aggiunta CLEAR impiegherà metodologie avanzate per la gestione dei rischi cyber, con un focus su modelli predittivi e intelligenza artificiale applicata alla sicurezza IT-OT.

netservice
Empowering Digital Evolution
Home | L'eccellenza italiana nel settore IT | Net Service | Net Service S.p.A.

AI per la creazione di dati sintetici: la piattaforma AINDO

L'impiego di dati sintetici è una soluzione che sta prendendo sempre più piede in svariati settori, come quello finanziario e medico, per evitare l'impiego di dati sensibili che potrebbero essere oggetto di un data-breach. La startup Aindo, in collaborazione con Obloo, ha prodotto una piattaforma in grado di generare dati iper-realistici, ma completamente sintetici grado di sostituirsi ai dati personali, permettendo di realizzare analisi di database sicuri e capaci di produrre risultati che rispecchiano la realtà.

I dati sintetici sono principalmente utilizzati nel settore finanziario per garantire prodotti su misura ai clienti e nel settore medico per velocizzare i trial clinici, ma trovano applicazione in numerosi altri ambiti, come nel settore del marketing, delle telecomunicazioni e dell'energia. In generale, l'impiego di dati sintetici non solo permette lo sviluppo di modelli descrittivi e predittivi evitando problemi di privacy, bias o insufficienza di dati disponibili, ma permette anche un grande risparmio economico alle aziende che optano per questa soluzione.

La creazione di un database interamente formato da dati sintetici è possibile grazie all'impiego dell'intelligenza artificiale: i dati sono infatti creati tramite l'AI generativa, essendo così più completi e sempre compatibili con i principali sistemi e formati utilizzati rispetto ai dati raccolti empiricamente. La piattaforma Aindo permette inoltre di visualizzare i dati in maniera intuitiva e user-centric grazie a dashboard e ad un interfaccia semplice, supportando tutti i tipi di formati per i dati organizzativi, indipendentemente dalla loro complessità. Aindo rispetta inoltre i requisiti di privacy-by-design, permettendo agli utenti un uso locale della piattaforma, rispettando tutte le misure tecniche ed organizzative relative alla privacy.

obloo
deepscover what matters

Obloo - About us

FogAtlas: un software la sicurezza dei dati nel Cloud Computing

Il Cloud Computing è una tecnologia ben consolidata che offre una varietà di servizi in diversi settori e per sua natura ha un approccio fortemente centralizzato che presenta alcune limitazioni: grazie ai dispositivi IoT una quantità enorme di dati viene prodotta in località remote e per consentirne l'elaborazione è necessario un trasferimento verso il Cloud centrale. Questo spostamento può generare problematiche in termini di inefficienza, disponibilità e robustezza, ma soprattutto in termini di privacy e sicurezza dei dati. FogAtlas è un software che ha l'obiettivo di gestire un'infrastruttura di Cloud Computing decentralizzata, in grado di fornire servizi vicino alle fonti dei dati e agli utenti, abbracciando il paradigma del Fog Computing.

FogAtlas porterà benefici principalmente ai proprietari di infrastrutture come provider cloud o gestori di reti di sensori che desiderano gestire in modo efficiente un'infrastruttura Fog Computing e a sviluppatori di applicazioni innovative, che vogliono sfruttare i vantaggi di un'infrastruttura distribuita sul territorio e vicina alle fonti di dati.

FogAtlas è una piattaforma software, basata su tecnologie Open Source, in particolare Kubernetes e Ansible, estese e integrate per orchestrare applicazioni *cloud-native* e supportare le operazioni in un ambiente Cloud Computing multi-livello, altamente distribuito, eterogeneo e decentralizzato. La piattaforma offre quindi le seguenti funzionalità: set-up, monitoraggio, gestione operativa, gestione dell'infrastruttura distribuita multi-tier, deployment automatizzato, allocazione delle risorse e posizionamento dei carichi di lavoro

Parole di tecnologia

Che cos'è il Fog Computing?

Il Fog Computing è un approccio che mira a estendere i concetti del Cloud Computing con l'obiettivo di offrire servizi e funzionalità cloud lungo l'intera infrastruttura che connette il cloud ai dispositivi IoTs. La raccolta dei dati avviene quindi il più vicino possibile ai dispositivi IoTs, mentre l'analisi si attua a livello del cloud, in modo da riscontrare una maggiore tutela della privacy e della sicurezza dei dati, questa tecnologia permette inoltre l'attuazione di risposte in tempo reale e bassa latenza, un uso della banda ottimizzato e una più alta tolleranza ai guasti.



Obloo - About us

SafeBot4Twin: un chatbot per la sicurezza dei dati sensibili

Il progetto SafeBot4Twin sviluppato da RBF Morph S.r.l. in collaborazione Livgemini S.r.l. e università di Roma Tor Vergata propone lo sviluppo di un nuovo un nuovo chatbot basato per controllare Medical Digital Twin costruiti mediante dati clinici e garantire la sicurezza delle informazioni sensibili sottostanti necessari per la loro creazione ed il loro utilizzo.

Il progetto nasce in risposta all'impiego sempre più diffuso dei gemelli digitali in ambito medico, i quali richiedono l'elaborazione di una grande quantità di dati sensibili per essere realizzati. L'obiettivo di SafeBot4twin è quello di fornire in modo autonomo un monitoring periodico e risk assesment, utilizzando algoritmi avanzati per analizzare e sintetizzare informazioni rilevanti, agendo come strumento di sicurezza user-friendly in grado di assistere personale non formato in operazioni complesse quali Vulnerability Assesment e pratiche di Remediation.

Il chatbot permetterà a tutti gli operatori di interagire con il Digital Twin in modo semplice e diretto per via della sua natura basata su Large Language Model (LLM), un'avanzata applicazione di intelligenza artificiale basata sulla comprensione e analisi del testo che sfrutta tecniche di deep learning per il proprio apprendimento, in modo da permettere agli utenti di interagire con il chatbot senza dover possedere nessuna capacità di programmazione.

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Progetti Finanziati - Cyber 4.0

Tutelare la riservatezza dei dati sensibili nella telemedicina: Health-e-Data

Moveax S.r.l. in partnership con Exprivia S.p.A. sta sviluppando Health-e-Data, un progetto incentrato sullo sviluppo ed implementazione di tecnologie volte a preservare la sicurezza e la riservatezza dei dati sensibili in applicazioni di telemedicina digitale avanzate.

Il progetto Health-e-Data, intende esplorare e validare elementi tecnologici innovativi essenziali a facilitare la gestione, lo scambio, e lo sfruttamento di dati sanitari – con particolare attenzione ai dati generati in un contesto di telemedicina e telemonitoraggio, mirando a consentire una mobilità dei dati sanitari tra diversi operatori e con il coinvolgimento di cittadini e pazienti, creando nuovi modelli di creazione di fiducia in grado di superare i limiti strutturali dei sistemi esistenti.

Il progetto intende inoltre validare dal punto di vista tecnico-scientifico l'utilizzo di algoritmi di intelligenza artificiale per facilitare la fruizione dei dati tramite processi di sintetizzazione, così da poterli mettere più facilmente a disposizione degli sviluppatori. Per garantire la sicurezza dei dati sanitari Healt-e-Data farà utilizzo di tecniche di intelligenza artificiale e della tecnologia blockchain.

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Progetti Finanziati - Cyber 4.0

Biosat MarketPlace: servizi satellitari on demand per la pubblica amministrazione

Biosat MarketPlace è un progetto in fase di sviluppo ideato da IPTSAT S.r.l. che mira a creare un sistema informativo satellitare per servizi on demand destinato e modellato sulle necessità della pubblica amministrazione.

Biosat MarketPlace ha come obiettivo quello di fornire un servizio, in primis la pubblica amministrazione locale e poi l'industria, finalizzato a colmare il divario tra la potenziale utilità dei prodotti derivati dall'Osservazione della Terra e le esigenze pratiche e operative di informazione espresse dalle Pubbliche Amministrazioni Locali italiane. Il progetto promuove quindi l'utilizzo di prodotti informativi derivati dall'osservazione della Terra, principalmente dalle missioni ESA/UE e dalla futura costellazione IRIDE, per aumentare la consapevolezza tra le comunità di utenti target dell'applicabilità dei servizi di osservazione della Terra nelle loro operazioni quotidiane.

Il progetto si propone quindi di utilizzare le nuove tecnologie per la creazione del sistema informativo Biosat Marketplace integrato con una serie di servizi predefiniti ed operativi per realizzare un processo sicuro, chiaro e rapido per la fornitura di servizi e dati a valore aggiunto alla PA.

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Progetti Finanziati - Cyber 4.0

HESI: un progetto per la salvaguardia dei dati satellitari

Il progetto HESI sviluppato da DIGIMAT S.p.A. in collaborazione con TrAI Group Italia S.r.l. mira alla creazione di un sistema avanzato per la gestione sicura di immagini satellitari mediante crittografia omomorfica.

L'obiettivo principale del progetto si riscontra nello sviluppo di un sistema software avanzato per la formattazione di prodotti satellitari, specificamente progettato per la gestione e l'elaborazione di immagini satellitari SAR (Synthetic Aperture Radar) e ottiche. Gli strumenti di osservazione satellitare sono infatti sostanziali per diversi settori produttivi: dalla finanza all'agricoltura, dai trasporti all'intelligence, passando per la connessione dati degli smartphone e l'Internet of Things. La sicurezza di questi strumenti è quindi fondamentale, poiché un cyber-attacco andato a buon fine potrebbe produrre ripercussioni disastrose in molti aspetti della vita quotidiana.

Questo sistema dovrà impiegare tecniche di crittografia omomorfica, un tipo di crittografia che permette la manipolazione di dati cifrati, consentendo così l'esecuzione di operazioni chiave senza la necessità di decriptare i dati. Questo approccio innovativo permetterà di eseguire una serie di operazioni fondamentali per la trasmissione e l'elaborazione dei dati satellitari, mantenendo sempre i dati in forma cifrata, garantendo così la massima sicurezza e riservatezza.

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Progetti Finanziati - Cyber 4.0

Proteggere i dati aziendali dai ransomware: il progetto DCS

Il progetto Distributed Content Security (DCS), guidato da Teleconsys S.p.A in collaborazione IOTA Foundation, Sapienza Università di Roma e Università Campus Biomedico mira a proteggere le aziende dagli attacchi ransomware.

L'obiettivo principale del progetto DCS è la protezione dei dati aziendali attraverso l'integrazione delle tecnologie IOTA, applicazioni nel contesto dell'Internet-of-Things-IoT e Inter Planetary File System (IPFS): la soluzione combina la sicurezza e prestazioni del registro distribuito IOTA con le capacità di archiviazione decentralizzata di IPFS, offrendo una protezione avanzata ed economicamente sostenibile per i dati applicativi.

L'innovazione che questa soluzione apporta consiste nel permettere la distribuzione di file su uno storage distribuito IPFS, accessibile tramite un servizio di gateway che supporta vari protocolli, fornito da un plug-in attivabile sui nodi del registro distribuito.

Parole di tecnologia

Che cos'è la tecnologia IOTA?

IOTA, che prende nome dalla lettera greca *iota* (ι), è un registro distribuito sviluppato per eseguire e tenere traccia delle transazioni, di valore o di dati, tra dispositivi e macchine nell'Internet-of-Things IoT. L'innovazione principale di IOTA è una rete di nodi utilizzata per confermare le transazioni, detta IOTA più efficiente e sicura delle blockchain solitamente utilizzate nelle criptovalute.

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Progetti Finanziati - Cyber 4.0

Sicurezza per le stazioni di ricarica dei veicoli elettrici: CyberGuardEV

TME – Test and Manufacturing Engineering S.r.l in partnership con Alfagreen Solution S.r.l. sta sviluppando un sistema integrato per la sicurezza informatica nelle stazioni di ricarica per veicoli elettrici detto CyberGuardEV.

Il progetto ha come principale obiettivo la realizzazione di un dispositivo elettronico innovativo in grado di rilevare attacchi side-channel per proteggere le stazioni di ricarica per veicoli elettrici. Le stazioni di ricarica sono infatti dei sistemi cyber fisici connessi alle reti di comunicazione per la gestione della stesse, tra le varie azioni di gestione si riscontrano: il logging e la trasmissione dei dati elettrici di funzionamento relativi alle operazioni di ricarica dei veicoli, come energia erogata e profili temporali, la gestione dell'interfaccia uomo-macchina e le transazioni economiche associate al relativo funzionamento.

Le stazioni di ricarica sono quindi sistemi connessi alla rete dati e alla rete elettrica che contengono e scambiano svariati dati, prestandosi come perfetto obiettivo per diverse superfici di attacco di tipo side-channel.

Parole di futuro

Che cos'è un attacco side-channel?

Con attacco side-channel si intende un tipo di attacco informatico che non ha come obiettico direttamente il software o i protocolli di sicurezza, ma mira a carpire "informazioni collaterali" che osserva dal sistema durante il suo funzionamento. Queste informazioni "collaterali" (side) possono essere: i tempi di esecuzione, il consumo energetico o emissioni elettromagnetiche o acustiche del sitema. Nel caso delle stazioni di ricarica, un attacco side-channel potrebbe mirare a intercettare dati sensibili durante le transazioni economiche, ricostruire il profilo di ricarica del veicolo o ancora alterare il comportamento della stazione monitorando il suo consumo elettrico.

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Progetti Finanziati - Cyber 4.0

SATML-B: sicurezza nelle tecniche di Machine Learning e analisi Big Data

Il progetto SATML-B coordinato da Datrix S.p.A è l'estensione di CybersecH, un'iniziativa finanziata da Cyber 4.0 e completata con successo nel febbraio 2023 e che ha portato allo sviluppo della piattaforma modulare AIA-Guard, che migliora la resistenza dei modelli AI agli attacchi avversarsi, dagli input malevoli e salvaguardia la privacy dei dati sensibili attraverso protocolli di Data Sanitization e Data Anonymization.

L'obiettivo del progetto SATML-B è quello di ampliare le funzionalità della piattaforma AIA-Guard portando il livello di maturità tecnologica (Technology Readiness Level – TRL) finale della piattaforma ad otto. Il TRL è infatti una scala per misurare la maturità di una determinata tecnologia e si misura da uno a nove, attualmente la piattaforma ha un TRL pari a sei, che sta a significare che la tecnologia è in fase di dimostrazione in un ambiente rilevante.

I miglioramenti alla piattaforma AIA-Guard verranno ottenuti attraverso tre principali iniziative strategiche e con forte potenziale commerciale. In primo luogo, verrà eseguita l'espansione dei moduli relativi agli adversarial attacks, successivamente verrà perfezionato il modulo di AI Shield, e infine verrà esteso anche il modulo di Data Sanitization & Anonymization.

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Progetti Finanziati - Cyber 4.0

ESII: un progetto per l'indagine tempestiva degli incidenti

Sharelock S.r.l. è una startup italiana nell'ambito della cybersecurity che si occupa di creare prodotti per l'intercettazione di anomalie comportamentali basate sull'intelligenza artificiale e intende sviluppare un sistema di investigazione preliminare sugli incidenti di sicurezza (Early Security Incident Investigation – ESII).

La soluzione si propone l'integrazione di un Large Language Model (LLM) specificatamente addestrato, capace di inserirsi in modo sinergico nei prodotti Sharelock Identity Threat Detection and Response (ITDR) e Sharelock Cloud Workload Protection (CWP) per effettuare investigazioni sugli alert di sicurezza che questi prodotti emettono.

Shearelock utilizza l'intelligenza artificiale generativa per una classificazione precisa dei dati, per l'identificazione delle anomalie e l'analisi, l'analisi delle minacce e una mitigazione proattiva del rischio, il progetto ESII permetterà un'ulteriore innovazione grazie all'implementazione della tecnologia LLM, che a sua volta renderà possibile far fronte alle sfide che la complessità delle minacce informatiche comporta, consentendo di condurre indagini dettagliate e tempestive su singole o gruppi di anomalie.

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Progetti Finanziati - Cyber 4.0

WISE PACK: proteggere l'industria farmaceutica dai cyber-attacchi

Wireless In-package Sensors to protect the Pharmaceutical Industry against cyber-physical attacKs – WISE PACK è un progetto sviluppato da Radio6Sense in partnership con GUNPOWDER finalizzato alla protezione dell'industria farmaceutica da attacchi informatici

Gli impianti farmaceutici e l'intera catena di approvvigionamento, alla stregua di altre infrastrutture critiche come i data center, le centrali energetiche, e le reti ICT, sono diventati ormai potenziali bersagli di attacchi cyber-fisici. Il progetto WISE PACK ha come obiettivo il contrasto e la prevenzione di questi fenomeni, attraverso lo sviluppo di una infrastruttura di monitoraggio e protezione contro le suddette minacce in grado di ribaltare i tradizionali paradigmi di monitoraggio.

La grande innovazione che WISE PACK porterà nell'industria farmaceutica si identifica nell'integrazione sinergica di sensori IoT, posizionati all'interno dell'imballaggio dei farmaci, e sistemi di Intelligenza Artificiale, in modo che lo stesso prodotto farmaceutico con il suo packaging sia in grado di identificare e segnalare gli effetti di attacchi al processo o di azioni di contraffazioni, registrando anomalie ambientali all'interno del microambiente della confezione, sia durante il processo di produzione che nelle successive fasi di conservazione e controllo qualità.

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Progetti Finanziati - Cyber 4.0

Asset Discovery: mappare i dispositivi OT per una difesa efficace

MON5 è una startup italiana che si occupa di proteggere le infrastrutture critiche da minacce esterne, garantendo la continuità operativa in una vasta gamma di settori produttivi, dalla manifattura alla produzione energetica, fino agli ambiti militare e logistico. Uno dei suoi prodotti è Asset Discovery, una piattaforma che consente di produrre un inventario completo e accurato di tutti gli asset aziendali.

Avere un inventario preciso di tutti gli asset è il primo passo da compiere per poter attuare una strategia di cybersecurity efficace, Asset Discovery permette infatti di avere una mappatura precisa e in tempo reale di tutti gli asset IoT connessi alla rete, offrendo un controllo totale sull'ambiente operativo e potenziando la difesa: la conoscenza accurata di ogni dispositivo permette infatti di identificare vulnerabilità nascoste e implementare protezioni mirate, riducendo drasticamente la superficie d'attacco. Un inventario dinamico di tutti i dispositivi OT consente inoltre di semplificare radicalmente i processi di conformità alle nuove direttive e normative.

Asset Discovery si basa sulla distribuzione strategica di sonde hardware all'interno degli impianti produttivi che consentono di identificare e classificare in tempo reale tutti i dispositivi IIoT, OT e i sistemi connessi IP, gestiti o non gestiti; la soluzione integra poi un ampio database di dispositivi OT, arricchendo i dati con informazioni tecniche aggiornate e dettagli specifici di ogni dispositivo. La piattaforma permette inoltre di analizzare il comportamento degli asset nel loro contesto operativo, riducendo significativamente gli avvisi falsi positivi e rendendo possibile l'associazione di ogni asset ad un profilo di rischio chiaro e aggiornato, permettendo di identificare vulnerabilità, criticità e priorità d'intervento a livello di dispositivo, zona o intero impianto, migliorando l'efficienza nella gestione della sicurezza.

MON5

mon5.it/discovery/

Identificare le vulnerabilità nelle infrastrutture critiche: MON5 Fortezza

MON5 Fortezza è un altro prodotto della startup MON5 che ha come obiettivo l'identificazione delle attività anomale nella rete OT di un'azienda, in modo da rilevare proattivamente le vulnerabilità che possono essere sfruttate durante un attacco informatico.

L'obiettivo di MON5 Fortezza è quello di fornire alle aziende una soluzione completa e sicura, per una gestione proattiva della sicurezza e in grado di fare da barriera anche verso gli insider threat. Il prodotto offre quindi un monitoraggio approfondito: esegue interrogazioni mirate sui dispositivi a bordo macchina per individuare e neutralizzare tempestivamente le minacce e assicura la continuità delle operazioni anche in presenza di quest'ultime, riducendo al minimo i tempi di inattività e garantendo la massima efficienza dei processi industriali.

La realizzazioni di questi obiettivi è possibile grazie all'istallazione di sonde periferiche in grado di rilevare attività malevole direttamente al livello dei macchinari, MON5 Fortezza è inoltre in grado di analizzare in tempo reale tutto il traffico di rete, utilizzando regole aggiornate per identificare e segnalare nell'immediato qualsiasi comportamento sospetto. La soluzione è inoltre flessibile e adattabile alle dimensioni e alla complessità di qualsiasi infrastruttura.

Parole di futuro

Che cos'è un insider threat?

Con il termine insider threat si intende un tipo di cyber-attacco che ha origine da uno o più individui che lavorano per l'organizzazione che viene minacciata, rendendo l'attacco più pericoloso e con più probabilità di andare a buon fine poiché questi individui hanno accesso ai network e sistemi interni.
Solitamente un insider threat può identificarsi in un ex-dipendente, un consulente, un business partner o in altri attori coinvolti che possono essere più o meno consapevoli del danno che stanno arrecando.

MON5

mon5.it/fortezza/

ToothPic: identità digitali non clonabili e sicurezza dei Big Data

ToothPic, azienda specializzata in cybersecurity e spinoff del Politecnico di Torino, ha sviluppato e brevettato una soluzione di autenticazione innovativa, in grado di garantire la sicurezza dell'identità digitale, l'affidabilità e la tracciabilità dei dati fin dalla loro origine. In contesti caratterizzati da un'elevata produzione di dati sensibili, è infatti essenziale poter associare in modo univoco ogni informazione al dispositivo che l'ha generata. ToothPic risponde a questa sfida trasformando la fotocamera di ogni smartphone in un'identità digitale non clonabile, utilizzabile per autenticare in modo sicuro l'accesso e certificare la provenienza dei dati.

Nel contesto odierno dominato dai Big Data, l'adozione di ToothPic consente un controllo avanzato sulla qualità e l'integrità delle informazioni, assicurando che ogni dato possa essere ricondotto alla sua origine. Questa tracciabilità è particolarmente strategica in settori come la sanità, la finanza e la pubblica amministrazione, dove la sicurezza, la conformità normativa sono requisiti essenziali: ToothPic si afferma quindi come una soluzione chiave per costruire ecosistemi digitali sicuri, affidabili e privacy-oriented.

Per raggiungere i suoi obiettivi di sicurezza, ToothPic sfrutta le imperfezioni uniche del sensore fotografico per generare credenziali sicure e impossibili da clonare: questo approccio permette di autenticare l'identità del dispositivo in modo trasparente e senza la necessità di hardware aggiuntivo, rendendo la tecnologia facilmente scalabile e integrabile nei sistemi esistenti. Oltre a rafforzare la sicurezza dei dati, ToothPic semplifica i meccanismi di autenticazione, proteggendo gli accessi e le comunicazioni digitali da minacce come phishing, spoofing e furti d'identità, rispettando la privacy: le credenziali generate non lasciano infatti tracce permanenti, poiché vengono elaborate localmente e distrutte senza essere archiviate a lungo termine.

toothpic

Toothpic – Unlock your smartphone's potential

Intesa Sanpaolo collabora con IBM nel testare soluzioni post quantistiche

Intesa Sanpaolo (ISP) e IBM hanno lavorato insieme eseguendo diversi test con le librerie crittografiche di IBM Research su due dei quattro algoritmi di crittografia post-quantistica selezionati dal National Institute for Standards and Technology (NIST) per il processo di definizione della standardizzazione futura: CRYSTALS-Kyber per la crittografia generale e CRYSTALS-Dilithium per le firme digitali. Nell'ultimo anno, tali librerie sono diventate parte del prodotto IBM Quantum Safe Remediator, che permette di implementare modelli quantum-safe basati sulle migliori pratiche e comprendere l'impatto potenziale sui sistemi e sulle risorse dovute all'adozione di soluzioni quantum-safe.

La collaborazione tra IBM e ISP sul tema quantum-safe, iniziata a fine 2022, è nata dalla necessità di ISP di anticipare i tempi nel proteggersi rispetto a un futuro computer quantistico, disponibile su larga scala, che potrebbe mettere a rischio l'attuale crittografia a chiave pubblica. ISP era consapevole della necessità di passare ad una crittografia sicura dal punto di vista quantistico e voleva capire fino a che punto l'uso della crittografia quantum-safe fosse fattibile e maturo, quali potessero essere gli impatti potenziali e la complessità per la futura adozione.

I test sono stati eseguiti utilizzando l'ambiente IBM Cloud, dove ISP ha potuto sperimentare diverse applicazioni degli algoritmi di crittografia quantum-safe, in gran parte supportati da componenti open-source. Una volta che il team di IBM ha distribuito l'ambiente di test, ha supportato il team di ISP in test sulle prestazioni con i seguenti scenari: client/server semplice, client/server tramite proxy in uscita, VPN e tra cluster Red Hat Openshift.

Basandosi sulla sua esperienza nella ricerca di algoritmi di crittografia post-quantistica, nel 2023 IBM ha annunciato la tecnologia e la roadmap per IBM Quantum Safe - un progetto che traccia le tappe fondamentali verso una tecnologia di sicurezza quantistica sempre più avanzata.

Intesa Sanpaolo collabora con IBM nel testare soluzioni post quantistiche

Intesa Sanpaolo e IBM proteggono le transazioni digitali: la Fully Homomorphic Encryption (FHE)

Intesa Sanpaolo (ISP) riconosce che la FHE ha il potenziale per supportare una strategia zero trust mantenendo i dati delle transazioni degli asset digitali dei clienti, i modelli che elaborano i dati e i risultati generati crittografati end-to-end, anche durante l'elaborazione. Questo approccio di sicurezza avanzato può proteggere da attacchi esterni e minacce interne che rubano proprietà intellettuale o informazioni sensibili, intenzionalmente o inavvertitamente. Intesa Sanpaolo monitora lo sviluppo di tecnologie emergenti che possano offrire una maggiore protezione per le transazioni di asset digitali.

Il Cybersecurity Lab di ISP aveva la necessità di sviluppare un sandbox per preservare la riservatezza delle informazioni riservate relative alle transazioni patrimoniali dei clienti durante l'elaborazione e nel sistema della banca.

Lo scenario scelto prevedeva di consentire a un cliente di eseguire una transazione in criptovaluta con una terza parte. La banca avrebbe approvato la transazione se la terza parte non fosse comparsa nella sua blacklist e se nel portafoglio del cliente fossero presenti fondi sufficienti. L'innovazione consiste nel fatto che i dati della terza parte e altri dettagli della transazione sono rimasti crittografati per tutta la durata della transazione. Utilizzando FHE, i dati crittografati della terza parte sono stati convalidati rispetto alla blacklist della banca e approvati o rifiutati senza esporre dati sensibili a nessuna delle parti coinvolte, migliorando la sicurezza e la privacy di tutti i partecipanti.

Con un'elaborazione end-to-end delle transazioni in meno di 22 secondi e una blacklist di 32.000 record, il progetto ha dimostrato in modo definitivo che FHE è adatto alla protezione delle transazioni digitali.

Intesa Sanpaolo and IBM secure digital transactions with fully homomorphic encryption

Fortgale: sicurezza personalizzata contro i cyber threats

Fortgale è un'azienda italiana specializzata nella difesa informatica avanzata e nella gestione dei cyber threats, che fornisce servizi su misura per la protezione del business, della proprietà intellettuale e del know-how, ad aziende operanti in settori diversificati quali trasporto marittimo, aereonautico, aerospace, manifatturiero, bancario, assicurativo.

Fortgale tramite il suo Security Operation Center (SOC) offre alle aziende una difesa continua 24/7, riducendo i rischi e assicurando la conformità con le normative in continua evoluzione in materia di sicurezza informatica. Fortgale analizza costantemente le tendenze globali nel cyberspazio, le tattiche e le tecniche degli attaccanti e le potenziali vulnerabilità per garantire un servizio sempre aggiornato ed efficace.

Fortgale fornisce servizi cyber adattati alle esigenze del cliente, quali: Managed Detection and Response (MDR): difende proattivamente gli asset aziendali, garantendo la continuità operativa e assumendo la piena responsabilità delle attività di Incident Response. Cyber Threat Intelligence: produce informazioni tempestive, concrete e pertinenti sulle minacce informatiche emergenti, insight operativi e allerte immediate. Monitoraggio del Deep e Dark Web: rafforza la postura complessiva di sicurezza delle aziende contro i rischi nascosti. Intelligence Feed: fornisce intelligence operativa sulle minacce informatiche emergenti, con un focus particolare su quelle dirette contro l'Europa, proponendo una selezione accurata di Indicatori di Compromissione (IOC), frutto di anni di osservazione e analisi approfondita delle infrastrutture offensive.

FORTGALE
CYBER GOVERNANCE & DEFENCE

Fortgale | Secure your business

Dilaxia: servizi su misura per la protezione delle aziende

Dilaxia è un ecosistema in continua evoluzione, con sedi in Italia e Albania, che trasforma le sfide digitali in soluzioni concrete, scalabili e personalizzate, costruendo tecnologia che funziona e crea valore reale per aziende e organizzazioni, partendo da software su misura all'AI, passando per l'IT support alla cybersecurity.

Tra in benefici che Dilaxia apporta ai suoi clienti si possono annoverare varie attività innovative in tutti le fasi del Cyber Risk Management: da servizi di Cyber Risk Assesment, passando per i servizi di prevenzione come Penetration Test e simulazioni di attacchi, servizi di monitoraggio come Business Continuity & Disaster Recovery e Incident Response, proponendo anche servizi di formazione e sensibilizzazione ai rischi cyber per i dipendenti delle aziende che lo richiedono.

L'innovatività e la forza dei servizi di Dilaxia risiede nella capacità di assistere a tutto tondo i propri clienti, come nel caso di una grossa azienda del territorio lombardo che si è rivolta a loro per attività di Incident Response e successiva Remediation: l'intera infrastruttura server del cliente era stata resa indisponibile, i dischi di tutte le macchine virtuali e fisiche erano stati cifrati e anche i repository di backup erano stati attaccati. In questo caso è stata determinante la preventiva predisposizione di snapshot a livello storage**,** una funzionalità e che ha permesso di ripristinare l'intera infrastruttura virtuale, per il recupero dei server fisici è stata invece fondamentale la preventiva implementazione del backup dei sistemi operativi sul provider cloud Microsoft Azure, che ha reso possibile di ripristinare i dati senza assecondare le richieste di pagamento da parte degli attaccanti. Le operazioni di Remediation sono poi state implementate tramite distribuzione di agenti EDR per controllo e analisi dei device in rete, supporto legale per determinare strategia ottimale di intervento sui sistemi, conservazione delle prove e attivazione comunicazione con i criminali per cercare di ottenere informazioni utili per ricostruire gli eventi, ripristino dei sistemi disponibili da storage snapshot e da backup cloud ed infine sostituzione delle credenziali amministrative sui sistemi, protezione delle connessioni VPN e introduzione politica di Multi-Factor Authentication.

YOUR DIGITAL GATE
dilaxia

Servizi di cybersecurity per aziende - Dilaxia

Le soluzioni Visa Protect in ambito autenticativo per Banche ed Istituzioni Finanziarie

Le soluzioni Visa Protect aiutano a prevenire le frodi lungo tutto il processo transazionale, garantendo una continuità nei flussi di pagamento. Tra queste, rientrano le soluzioni Visa Protect in ambito Autenticativo, ovvero quelle soluzioni che consentono un'autenticazione del cliente fluida mantenendo il processo di pagamento senza frizioni. Tra le soluzioni Visa Protect in ambito Autenticativo, rientrano gli score che utilizzano i dati Visa per identificare la rischiosità di una transazione. Tra questi menzioniamo:

- Visa Provisioning Intelligence (VPI) - utilizza il machine learning per valutare in tempo reale, tramite l'attribuzione di uno score, il rischio di richieste di token fraudolente, aiutando le istituzioni finanziarie a prendere decisioni informate sull'approvazione o il rifiuto delle richieste di provisioning

- Visa Protect Authentication Intelligence (VPAI) - attraverso l'analisi dei dati e l'utilizzo dell'Artificial Intelligence, assegna uno score a ciascuna richiesta di autenticazione. Questo score indica il livello di rischio associato alla transazione, aiutando gli emittenti a prendere decisioni più informate sull'approvazione o meno della stessa, riducendo i falsi positivi, migliorando il tasso di approvazione e consentendo di identificare eventuali frodi.

- Visa Consumer Authentication Services (VCAS) - sfruttando la potenza dell'intelligenza artificiale, il Visa Consumer Authentication Service (VCAS) fornisce uno score di rischio in tempo reale e network agnostic. VCAS consente ai clienti di ridurre le frodi e i falsi declini, permettendo così decisioni di autenticazione più intelligenti e sicure e una migliore esperienza per il titolare della carta.

Visa, una società leader nei pagamenti digitali | Visa

Visa Protect Authentication Intelligence (VPAI)

Visa Protect Authentication Intelligence utilizza quindi l'intelligenza artificiale per analizzare le caratteristiche transazionali e attribuire uno score di rischio alle transazioni carta non presente in fase autenticativa con lo scopo di ridurre le frodi senza aumentare gli abbandoni al carrello.

In Europa, lo score VPAI aiuta le banche emittenti a soddisfare i requisiti per poter richiedere le esenzioni di Transaction Risk Analysis (TRA) previste dall'articolo 18 paragrafo 3 della normativa PSD2, aiutando quindi a ridurre le richieste di challenge per le transazioni a basso rischio di frode.

Un caso reale, osservato su territorio Europeo, fa riferimento a un emittente con alti livelli di frode di abbandono del carrello su e-commerce. Per migliorare queste performance, l'emittente ha avviato una collaborazione con Visa implementando lo score VPAI con l'obiettivo di bilanciare la challenge rate (il numero di transazioni per le quali viene richiesto un ulteriore passaggio di verifica al cliente come l'inserimento di un codice o l'autenticazione biometrica) e il numero di frodi.Dopo i primi 4 mesi di utilizzo, l'emittente ha rilevato una riduzione del 25% nel Tasso di Abbandono e un 3.3% di miglioramento nell'Authentication Success Rate, miglioramento che ha garantito un utilizzo dello score a lungo ter

Visa, una società leader nei pagamenti digitali | Visa

Le tecnologie abilitanti per la cybersecurity nel Centro Nazionale di Ricerca in HPC, Big Data e Quantum Computing

Il Centro Nazionale di Ricerca in HPC, Big Data e Quantum Computing nel suo Spoke dedicato alle innovazioni in ambito quantum computing, ossia lo Spoke 10 - Quantum Computing coordinato dal Prof. Paolo Cremonesi (PoliMi) in collaborazione con il Prof. Simone Montangero (UniPD), si possono riscontrare la maggior parte dei progetti finanziati da ICSC in ambito di cybersecurity.



Figura 8: Logo dello Spoke 10 di ICSC capofila nei progetti in ambito cybersecurity

Lo Spoke 10 si occupa di studiare le enormi potenzialità in termini di velocità e gestione dei dati del quantum computing. I calcolatori quantistici hanno, infatti, la capacità di risolvere problemi complessi che nessun computer classico potrebbe risolvere in un tempo ragionevole, potenzialità nota come "supremazia quantistica".

Tuttavia, nonostante le alte e crescenti aspettative verso questa nuova tecnologia, soprattutto in considerazione dei potenziali impatti nei vari campi di applicazione e dei nuovi modelli di business che ne conseguiranno, lo sviluppo di applicazioni di quantum computing è ancora distante da una piena maturità tecnologica.

Tra le principali sfide che ostacolano un utilizzo pratico dei calcolatori si enumerano l'incertezza dell'affidabilità dei componenti e la complessità di programmazione, lo Spoke 10 si pone quindi come obiettivo l'ideazione e la sperimentazione di soluzioni per arginare queste difficoltà.

Lo Spoke 10 opererà secondo tre linee di ricerca: la prima consiste nella realizzazione di applicazioni che sfruttino i calcolatori quantistici come acceleratori per risolvere problemi altrimenti insolubili; la seconda si focalizza sulla realizzazione di strumenti hardware e software che facilitino la programmazione dei calcolatori quantistici e la loro interoperabilità con i calcolatori tradizionali; infine si cimenterà nella progettazione di computer quantistici di grandi dimensioni e scalabili.

Tutte queste applicazioni e innovazioni relative al quantum computing possono apportare enormi benefici nel settore della cybersecurity, declinata in vari campi, come quello finanziario o quello delle comunicazioni, come si vedrà in alcuni dei progetti presentati nella sezione seguente, ideati e sviluppati nell'ambito dello Spoke 10. Il quantum computing è infatti una tecnologia potente in grado di apportare benefici in tutte le fasi del cyber risk management, partendo dall'individuazione delle vulnerabilità, la valutazione del rischio, la prevenzione, la risposta e la mitigazione dei cyber-attacchi.

Il progetto CCO: il quantum computing svela le vulnerabilità della crittografia odierna

Il progetto CCO - Cybersecurity and Combinatorial Optimization si sviluppa all'interno dello Spoke 10 dell'ICSC e, sotto la guida di Sogei in partnership con Autostrade per l'Italia, IFAB, Intesa Sanpaolo, Università di Bologna e Università di Padova, si pone l'obiettivo di dimostrare che i computer quantistici possono decifrare un messaggio protetto dalla crittografia a chiave simmetrica/asimmetrica RSA.

All'interno del progetto viene simulato un attacco quantistico ad una comunicazione crittografata secondo il protocollo RSA (Rivest-Shamir-Adleman). Questo protocollo è uno degli algoritmi di crittografia più diffusi, è a chiave pubblica e si basa sulla difficoltà computazionale della fattorizzazione di numeri primi dal valore elevato. Questa tipologia di crittografia è ritenuta sicura contro gli attacchi cyber "classici", provenienti da computer tradizionali, ma gli attacchi provenienti da computer quantistici potrebbero essere in grado di forzare la crittografia RSA.

L'obiettivo finale del progetto CCO è quindi quello di mettere in luce questa vulnerabilità, mettendo in atto un attacco quantistico che considera gli approcci di Quantum Annealing, ovvero un metodo di calcolo quantistico volto a risolvere problemi di ottimizzazione e ricerca trovando il minimo di una funzione di costo, e l'algoritmo di fattorizzazione variazionale quantistica (VQF), un tipo di algoritmo basato su circuiti quantistici variazionali (VQC) e progettato per la fattorizzazione di numeri interi.

Il progetto produrrà quindi nuova conoscenza nel settore della prevenzione ai "Data Breach", ovvero i furti di dati, sviluppando tecnologie innovative al fine di comprendere i limiti e i vettori degli attacchi futuri.

sogei

IFAB
INTERNATIONAL FOUNDATION
BIG DATA AND ARTIFICIAL INTELLIGENCE
FOR HUMAN DEVELOPMENT

autostrade per l'italia

INTESA SANPAOLO

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Migliorare la reattività agli attacchi grazie al machine learning: il progetto SCP

SCP - Serial Code Porting on HPC & Quantum Computing è un progetto sviluppato all'interno dello Spoke 3 dell'ICSC, coordinato da Sogei in collaborazione con il Politecnico di Milano, l'università Milano Bicocca e l'Università di Roma Tor Vergata; l'obiettivo finale di questo progetto si può riscontrare nella creazione di un sistema basato su algoritmi di Machine Learning per la prevenzione degli attacchi informatici.

Per raggiungere questo scopo, SCP si propone di riscrivere algoritmi di ML, già disponibili nelle loro versioni Open Source, in un linguaggio adatto al super computing (HPC) e in moduli compatibili con architetture basate sulla computazione quantistica.

Ciò è necessario poiché ambienti basati sul quantum computing o HPC potrebbero permettere risposte migliori e in tempo reale ai cyber-attacchi, aumentano la capacità reattiva, fattore fondamentale nel settore della cybersecurity.

Il progetto si concentra quindi non solo nell'utilizzo di algoritmi nei campi dell'HPC e del quantum computing, ma si focalizza anche nella creazione di una metodologia per la riscrittura sistematica degli algoritmi di machine learning rilevanti per le attività aziendali e in attività di clustering, svolte all'interno di architetture HPC, degli algoritmi utilizzati nel settore di ricerca e sviluppo.

SCP mira quindi ad avere un impatto concreto e immediato per le aziende e i privati nella loro capacità di risposata agli attacchi cyber, configurandosi anche come un importante laboratorio per la ricerca e lo sviluppo di nuove applicazioni del Machine Learning in ambito quantistico e HPC.

sogei

POLITECNICO MILANO 1863

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Fraud Detection: migliorare la sicurezza finanziaria grazie al quantum computing

All'interno dello Spoke 10 si colloca anche il progetto Fraud Detection – FD guidato da Intesa Sanpaolo affiancata da INAF, Politecnico di Milano, Università di Roma "Sapienza", Università degli studi di Roma "Tor Vergata", Università degli Studi di Firenze, e Università degli Studi di Padova, che punta ad affrontare la tematica della rilevazione delle frodi bancarie esplorando gli utilizzi del calcolo quantistico.

Le frodi bancarie vengono infatti sempre più spesso attuate tramite cyber-attacchi, rilevare le transazioni anomale risulta quindi essenziale per garantire l'integrità dell'intero sistema finanziario.

L'identificazione di queste transazioni fraudolente con carte di credito è tipicamente eseguita utilizzando tecniche di Machine Learning (ML) e Deep Learning (DL), l'innovazione di questo progetto si trova quindi nella proposta di utilizzare diverse versioni quantistiche di questi approcci tradizionali.

Un approccio quantistico nell'analisi delle carte di credito e dei documenti finanziari potrebbe offrire un significativo aumento della velocità di elaborazione, andando a migliorare la qualità dei risultati.

Fraud Detection non mira però ad escludere i metodi tradizionali di ML e DL, ma al contrario si propone di continuare ad utilizzarli per confrontarne l'efficacia delle prestazioni rispetto a quelle ottenute con metodi di calcolo quantistico, in modo da poter determinare vantaggi e svantaggi di ciascun approccio.

La valutazione comparata è infatti essenziale per poter valutare ambiti concreti di applicazione e le tipologie di problematiche che si prestano in modo migliore ad un approccio puramente quantistico, migliorando la sicurezza dei circuiti bancari.

Il Federated Learning come assicurazione per la privacy: il progetto FLF

Sempre a riguardo di cybersicurezza in ambito finanziario lo Spoke 1 sviluppa il progetto FLF – Federated Learning Finance, guidato da intesa Sanpaolo in partnership con l'università del Salento e l'Università di Torino.

Il progetto mira a integrare la necessità di preservare la privacy dei clienti finanziari, garantendo così la conformità normativa dei dati sensibili, con il sempre crescente impiego di modelli di apprendimento automatico e di AI in ambito finanziario. La risposta a questa esigenza si riscontra nel federated learning (apprendimento federato), ovvero una tecnica di apprendimento automatico che consente di addestrare modelli AI senza trasferire i dati grezzi a un server centrale, in modo da garantire sicurezza e privacy senza dover rinunciare a tutti i benefici di prestazione dell'apprendimento automatico.

Federated Learning Finance mira quindi a diffondere la conoscenza sulle tecniche di federated learning e a promuoverne l'adozione nel sistema bancario. Il progetto consiste quindi nella creazione di un sistema di apprendimento federato volto all'identificazione di entità nominate nelle quantità massive di dati, come trasferimenti bancari SEPA e SWIFT, generate da milioni di attori nazionali e internazionali.

Verranno quindi sviluppate tecniche federate per un pipeline di elaborazione del linguaggio naturale per il riconoscimento di entità nominate (Name Entity Recognition, NER), ovvero il processo di identificazione di entità specifiche all'interno di un testo, per la risoluzione delle co-referenze (Coreference resolution, CR), ovvero la determinazioni di quali pronomi in un testo si riferiscono alla stessa entità nominata, ed infine per il collegamento di entità denominate (Named Entity Linking, NEL), che consiste nel processo di collegamento tra entità nominate all'interno di un testo e fonti di conoscenza esterne, al fine di arricchire il contesto.

Questi compiti saranno affrontati tramite l'adattamento di Large Language Models su dati specifici del dominio per eseguire l'etichettatura delle sequenze per NER e utilizzando l'output di questo modulo per informare e migliorare i modelli per CR e NEL.

INTESA SANPAOLO

UNIVERSITÀ DEL SALENTO

UNIVERSITÀ DI TORINO

HF: identificazione dei guasti nei sistemi HPC per prevenire vulnerabilità

HF - Methods for the detection and identification of hardware faults in HPC systems for AI applications è un progetto coordinato da Intesa Sanpaolo in collaborazione con il politecnico di Torino e sviluppato nel contesto dello Spoke 1 e mira a sviluppare tecniche efficienti per l'identificazione di guasti hardware nei sistemi HPC, con particolare attenzione per le architetture utilizzate per l'esecuzione di applicazioni AI.

Attualmente, i sistemi di super calcolo HPC, rappresentano infrastrutture strategiche in numerosi ambiti di applicazione e la loro crescente complessità e l'evoluzione tecnologica dei dispositivi elettronici aumenta la possibilità del verificarsi di guasti hardware, che possono rappresentare una vulnerabilità sfruttabile da eventuali attacchi cybernetici, soprattutto tenendo conto del fatto che i sistemi HPC sono sempre più utilizzati nell'ambito finanziario. Inoltre, tali malfunzionamenti possono interferire con le applicazioni di AI, spesso coinvolte in processi critici.

Per questi motivi appare dunque fondamentale l'implementazione di meccanismi efficienti ed intelligenti per l'identificazione tempestiva di questi guasti, il progetto HF sviluppa infatti attività volte alla creazione di tecniche efficienti e specializzate al riconoscimento di guasti hardware nei sistemi HPC durante la fase operativa, con attenzione per processori, memorie e acceleratori di hardware utilizzati per l'esecuzione di applicazioni di intelligenza artificiale.

Il progetto non cura solo la parte tecnica, ma si occupa anche di valutare il costo e la facilità di integrazione delle tecniche proposte nei flussi esistenti, includendo l'utilizzo di test case appropriati, eventualmente forniti da Intesa Sanpaolo.

INTESA SANPAOLO

UNIVERSITÀ DI TORINO

Megatrend e segnali deboli collegati alle sfide nella cybersecurity

In questa sezione esploreremo i trend più significativi e le innovazioni emergenti che stanno plasmando la cybersecurity a livello globale. Analizzeremo quattro aree strategiche destinate a ridefinire il nostro futuro: il megatrend che vede una diffusione di tecniche di cyberwarfare e information warfare, i nuovi sviluppi in ambito quantistico che vanno ad intaccare la sicurezza della crittografia tradizionale, l'evoluzione del concetto di sicurezza nella Smart Cities, non solo per la salvaguardia del dato ma anche per la sicurezza dei cittadini ed infine un trend emergente riguardante i crowdsourced cyberattacks.

Questi trend non rappresentano semplici adattamenti, ma vere e proprie trasformazioni sistemiche che determineranno il modo in cui vivremo, investiremo e produrremo nei prossimi decenni.

Armi cibernetiche e information warfare: nuovi pericoli

La sicurezza informatica appare tra i 20 megatrend costantemente monitorati dall'Italian Institute for the Future, il quale ne evidenzia le recenti sfide mettendo in guardia sui pericoli della *cyberwarfare* e dell'*information warfare*.

Il cyberwarfare, detto anche guerra cibernetica, è diventato uno dei temi prevalenti nella sicurezza internazionale, soprattutto da quando, ai più "tradizionali" attacchi cibernetici, si è aggiunto il dominio dell'information warfare, ovvero la guerra d'informazione condotta attraverso la manipolazione dell'opinione pubblica in rete, attraverso fake news, propaganda, disinformazione e deepfake.

Focus: Parole di Futuro

Cos'è un Megatrend?

I megatrend sono grandi forze trasformative che hanno un impatto profondo e duraturo sulla società, l'economia, l'ambiente e la tecnologia. Sono tendenze di lungo periodo (tipicamente decenni) che influenzano significativamente molteplici aspetti della vita umana e dei sistemi economici.
Le caratteristiche principali dei megatrend sono:

- Durata pluridecennale
- Impatto globale o su vaste aree geografiche
- Effetti trasversali su più settori e ambiti
- Capacità di modificare strutturalmente comportamenti e sistemi

La guerra cibernetica è diventata un pericolo reale solo in tempi recenti, contestualmente all'evoluzione delle infrastrutture di Internet come essenziali per le attività di comando, controllo, comunicazioni e intelligence, con la crescente diffusione di "armi cibernetiche", ovvero dispositivi o un qualsiasi insieme di istruzioni informatiche volte a danneggiare illecitamente un sistema informatico o telematico avente carattere di infrastruttura critica. Il Dipartimento della Difesa americano classifica, inoltre, le *cyber operation* in tre tipologie: i *computer network attack* (CNA): finalizzati ad alterare o distruggere le informazioni; le operazioni

di *computer network exploitation* (CNE): raccolgono dati da una rete di un obiettivo; le operazioni di *computer network defence* (CND): azioni di carattere difensivo per rilevare attività non autorizzate nei sistemi informativi e respingere le minacce.



Figura 9: . Immagine generata tramite strumenti di IA Generativa. Credits: Osservatorio sulle tendenze e le applicazioni del Supercalcolo.

La difesa da minacce cibernetiche è diventata quindi la massima priorità degli Stati, soprattutto perché la cyberwar rappresenta la tipologia perfetta di "guerra asimmetrica", con azioni anche devastanti che possono essere portate a termine da gruppi terroristici anche poco strutturati, questo tipo di azioni aumentano inoltre velocemente la portata del danno potenziale, per cui ciò che preoccupa maggiormente per il futuro è soprattutto il rischio connesso all'Internet of Things, con la progressiva messa in rete di dispositivi di ogni tipo, dagli assistenti vocali domestici ai computer che controllano infrastrutture critiche.

Attualmente gli attacchi si stanno spostando verso i *cloud*: i nuovi attacchi non sono infatti più orientati a infettare le singole macchine, ma a colpire i database online, dove diventa più facile rubare i dati. Rendere invulnerabile agli attacchi di *cyberwar,* e in generale agli hacker, questa tipologia di sistemi è diventata una priorità: l'obiettivo è quello di sviluppare protocolli di crittografia quantistica, che renderebbero impossibile a potenziali intrusi di rubare dati.

L'*information warfare*, pur apparentemente meno pericolosa, è un fenomeno radicato nella quotidianità che comprende tecniche come azioni di propaganda, influenza e disinformazione online, in particolare sui social media, la produzione e diffusione di video e audio falsi (*deep fake*) e la creazione di profili falsi. Questo fenomeno ha un forte impatto sociale e politico, inoltre, se abbinato alle minacce descritte nei paragrafi precedenti, la pericolosità dei suoi effetti aumenta in maniera esponenziale.

La cybersicurezza e le tecnologie quantum: la nascita della crittografia post-quantistica

Tra i fenomeni emergenti di cui vengono individuati *weak signals* (Segnali deboli), nel report della Commissione Europea *Weak Signals in science and Technologies - 2024. Technologies at an early stage of development that could impact our future*,

vengono segnalati i recenti sviluppi nell'ambito di ricerca del quantum computing associato alla crittografia. I progressi nel settore del quantum computing sono già tangibili in diverse aree applicative: per quanto concerne la cybersicurezza la declinazione più pertinente è la necessità di sviluppare una crittografia post-quantistica, in quanto queste recenti evoluzioni renderanno la crittografia tradizionale sempre meno resistente ai cyber-attacchi e più facilmente decifrabile. Per questi motivi è importante cogliere i segnali deboli che preannunciano tale fenomeno e agire prima che queste eventualità si verifichino in modo dirompente, anticipando quindi gli sviluppi più pericolosi lavorando attivamente per la creazione di una crittografia post-quantistica, resistente anche a questo tipo di attacchi.

A livello globale gli Stati Uniti sono considerati pionieri nella crittografia post-quantistica, con programmi come la National Quantum Initiative (NQI) e importanti aziende che promuovono e attuano lo sviluppo di hardware e software per il calcolo quantistico, posizionando gli USA in prima linea nell'innovazione quantistica nel settore privato. Anche la Cina è un forte concorrente nella ricerca quantistica, con il governo cinese che finanzia programmi con piani innovativi nella distribuzione di chiavi quantistiche, nella crittografia post-quantistica e nei satelliti per comunicazioni sicure. L'Europa adotta invece un approccio collaborativo, volto a unire gli Stati membri dell'UE sotto il programma Quantum Flagship, che sostiene la ricerca in vari campi quantistici, come il calcolo quantistico, la comunicazione quantistica e la simulazione quantistica.

Focus: Parole di Futuro

Cos'è un Segnale debole?

I segnali deboli sono indizi o tendenze emergenti che, sebbene inizialmente poco visibili o non ancora pienamente sviluppati, possono anticipare cambiamenti significativi in un settore, un mercato o una società.

Caratteristiche dei segnali deboli sono:

- Bassa visibilità iniziale: non sono ancora mainstream e potrebbero essere trascurati da molti;
- Crescita potenziale: se osservati nel tempo, possono rafforzarsi e diventare trend dominanti;
- Ambiguità: non è sempre chiaro se e come influenzeranno il futuro;
- Multidisciplinarità: possono provenire da settori diversi e avere implicazioni trasversali.

Individuare i segnali deboli richiede un'attenta osservazione delle dinamiche di mercato, delle ricerche scientifiche, dei comportamenti sociali e delle innovazioni tecnologiche, unendo dati quantitativi e qualitativi per intercettare il futuro prima che diventi evidente.

A livello nazionale l'ACN, nella sua *Relazione Annuale al Parlamento 2024* ha segnalato i pericoli legati agli sviluppi quantistici, evidenziando la necessità restare al passo con le tecniche di crittografia post-quantistica e citando anche ad un documento informativo pubblicato nel luglio 2024, dal titolo *Crittografia post-quantum e quantistica: preparazione alla minaccia quantistica*, che riassume la situazione attuale sul quantum safe e affronta il problema della minaccia quantistica, analizzando anche alcuni degli sviluppi internazionali in materia.

La cybersicurezza nelle Smart Cities: protezione dei dati e non solo

La crescente digitalizzazione di processi e servizi e il massiccio impiego di dispositivi connessi (IoTs), in special modo nell'ambito urbano, hanno determinato l'allargamento esponenziale della superficie digitale attaccabile: sempre più città si stanno infatti dotando di soluzioni smart che digitalizzano settori chiave ed infrastrutture critiche, trasformandosi nel perfetto bersaglio di cyber-attacchi.

La segnalazione di questa nuova minaccia trova spazio nella *Relazione Annuale al Parlamento 2024* di ACN, che presenta un sunto delle principali tecniche di attacco e della tipologia di vittime presenti sul territorio nazionale. Nel 2024 gli eventi riguardanti la cybersecurity sono aumentati del 40% rispetto al 2023 e sono per la maggior parte volti al furto di dati e diretti verso le PA, sia a livello locale che centrale, come si può osservare nella Figura 10.

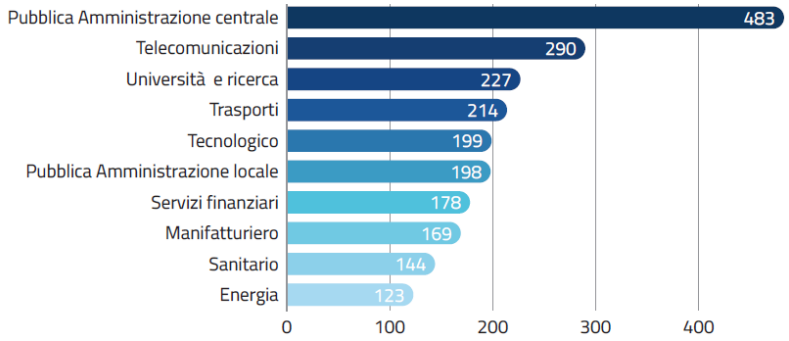


Figura 10: Vittime di eventi cyber trattati nel 2024 per settore target (Credits: Relazione Annuale al Parlamento 2024, ACN https://www.acn.gov.it/portale/relazione-annuale/2024)

Le Pubbliche Amministrazioni sono infatti detentrici di una grande quantità di dati sensibili, non sempre debitamente protetti, che vengono al giorno d'oggi raccolti e analizzati per scopi sempre più vari.

Scendendo maggiormente nel dettaglio delle tipologie di attacchi, l'ACN riporta come minaccia preponderante la *Distributed Denial Of Service* (DDoS), seguita dall'*information disclosure* e dal *brand abuse* (l'utilizzo di loghi e immagini istituzionali, solitamente ai fini di *phishing*). L'Agenzia segnala inoltre la rilevanza del *ransomware* che, pur rappresentando una moderata minaccia in termini di eventi verificati, ha impatti estremamente rilevanti: quasi nella totalità dei casi provoca l'indisponibilità prolungata dei dati con conseguenze importanti sull'operatività della PA o impresa colpita.

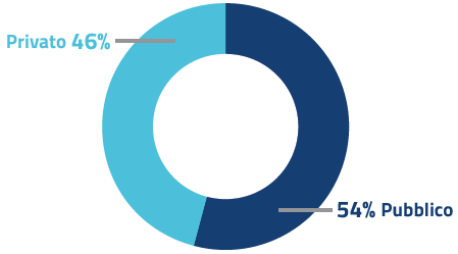


Figura 11: Eventi DDoS per tipologia di vittima (Credits: Relazione Annuale al Parlamento 2024, ACN https://www.acn.gov.it/portale/relazione-annuale/2024)

Anche considerando solo i soggetti vittime di DDoS, come si osserva nella Figura 11**Errore. L'origine riferimento non è stata trovata.**, si rileva una prevalenza di obiettivi pubblici: i settori più colpiti sono risultati quello dei trasporti, le Pubbliche Amministrazioni centrali e i servizi finanziari, tutti settori critici e di grande importanza per la salvaguardia della sicurezza dei cittadini.

Mantenendo il focus sulle PA, dopo il DDoS le altre forme di attacco maggiormente impattanti riscontrate sono: il *brand abuse*, seguito da azioni mirate alla compromissione dei dati, tra cui spiccano casi di esposizione non autorizzata (*information disclosure*) ed esfiltrazione di dati, spesso riconducibili a *ransomware* e malware. Nella Figura 12 si può invece osservare la distribuzione degli eventi cyber nei settori della Pubblica Amministrazione.

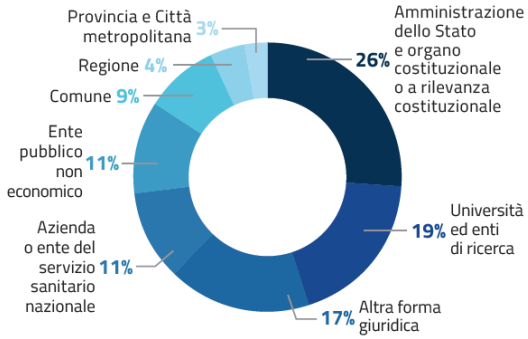


Figura 12: Distribuzione degli eventi cyber nei settori della Pubblica Amministrazione (Credits: Relazione Annuale al Parlamento 2024, ACN https://www.acn.gov.it/portale/relazione-annuale/2024)

La pericolosità di questi attacchi non si ferma ai danni relativi al furto o alla manomissione di dati, ma un attacco di tipo DDoS a un'infrastruttura critica, come una centrale elettrica, un ospedale, al sistema di trasporto pubblico o al sistema di controllo del traffico può avere conseguenze catastrofiche per la sicurezza delle comunità: la manomissione o l'interruzione prolungata dei servizi di una qualsiasi di queste infrastrutture potrebbe minare pericolosamente la sicurezza fisica dei cittadini, nei casi più estremi provocando anche danni irreparabili alla salute o conseguenze più gravi.

Crowdsourced Cyberattacks: un pericolo che amplia i confini geografici di un conflitto

Tra i trend classificati come "strengthening" presenti nella piattaforma Futures Platform, piattaforma realizzata da esperti nel settore dei *Future Studies*, si riscontra il fenomeno dei Crowdsourced Cyberattacks che consiste nel reclutamento di civili e gruppi di hacker criminali per attacchi informatici da parte di governi nazionali.

Questa tendenza consente agli individui di tutto il mondo dii partecipare a conflitti militari al di fuori della propria regione di origine, confondendo sia i confini legali che il confinamento geografico del conflitto; ad oggi gli attacchi informatici Crowdsourced sono stati per lo più atti semplici, come gli attacchi di negazione del servizio distribuito, ma l'ascesa di piattaforme di messaggistica anonima renderanno l'affiliazione tra gruppi hacker e nazioni sempre più comuni.

Queste attività mettono alla prova il diritto internazionale umanitario, rendendo più nebulosa la distinzione tra combattenti e civili, con il potenziale di portare a cambiamenti profondi nel panorama legale della guerra. Nel 2023, la Corte Penale Internazionale ha infatti affermato la sua giurisdizione sulla guerra informatica, suggerendo il potenziale per futuri precedenti che potrebbero ridefinire l'interpretazione delle leggi di guerra riguardo ai crimini informatici.

Bibliografia

A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Yuchong Li, Qinghui Liu, Energy Reports, Volume 7, 2021, Pages 8176-8186, https://doi.org/10.1016/j.egyr.2021.08.126.

ACN, Relazione Annuale al Parlamento 2024: Relazione annuale 2024 - ACN

Cyber Insurance – Models and Methods and the use of Ai, ENISA Research and Innovation Brief: Cyber Insurance - Models and methods and the use of AI | ENISA

Cyber Resilience Act: Cyber Resilience Act | Shaping Europe's digital future

CyberSec2025: CyberSec2025 AI, Spionaggio e Geopolitica: il nuovo mondo della Cybersecurity

Cybersecurity threats in the age of IoT: A review of protective measures; Amoo et al., 2024, International Journal of Science and Research Archive, 2024, 11(01), 1304–1310, https://doi.org/10.30574/ijsra.2024.11.1.0217n

Direttiva NIS2: Direttiva NIS 2: nuove norme sulla cibersicurezza delle reti e dei sistemi informativi | Plasmare il futuro digitale dell'Europa

ENISA, 2024 Report on the State of Cybersecurity in the Union: 2024 Report on the State of the Cybersecurity in the Union | ENISA

Fondazione SERICS: Fondazione SERICS – SEcurity and RIghts in the CyberSpace

Futures Platform: Futures Platform

Megatrend Hub, Italian Institute for the Future: I 20 megatrend globali che monitoriamo – Italian Institute for the Future

New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient: New EU Cybersecurity Strategy

Strategia Nazionale di Cybersicurezza 2022-2026: Strategia Nazionale di Cybersicurezza - ACN

Weak signals in science and technologies 2024: Weak signals in science and technologies 2024 - Publications Office of the EU


iFAB
INTERNATIONAL FOUNDATION
BIG DATA AND ARTIFICIAL INTELLIGENCE
FOR HUMAN DEVELOPMENT


bi-rex
Big Data Innovation & Research Excellence


POLITECNICO
MILANO 1863
SCHOOL OF MANAGEMENT


osservatori.net
digital innovation


netservice
Empowering Digital Evolution


CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER


MON5


YOUR DIGITAL GATE
dilaxia


IBM


obl
deepscover what matters


FORTGALE
CYBER GOVERNANCE & DEFENCE


toothpic


VISA

r citare il report

Osservatorio sulle tendenze e le applicazioni del Supercalcolo (2025). "Osserv-azioni su… CYBERSECURITY. Tendenze e applicazioni del Supercalcolo, Big Data e Quantum Computing". www.osservatorio.supercomputing-icsc.it

In concomitanza con il report, l'Osservatorio organizza un **webinar** sullo stesso tema. Il webinar ospita esperti, ricercatori e professionisti dell'innovazione che si interessano al tema in oggetto, per condividere casi d'uso e applicazioni future con la community.

Iscriviti o riguarda il webinar su
https://osservatorio.supercomputing-icsc.it/eventi/live-webinar-osserv-azioni-su-cybersecurity/

Realizzato e gestito da IFAB (International Foundation Big Data and Artificial Intelligence for Human Development), l'Osservatorio ha un focus privilegiato sulle PMI, sulle Pubbliche Amministrazioni e sulle Comunità.

L'attività dell'Osservatorio consiste nel mappare le più avanzate innovazioni tecnologiche, elaborare scenari futuri per lo sviluppo degli ecosistemi della ricerca e dell'innovazione e creare occasioni di incontro per i membri di questi ecosistemi.

Leggi questo e altri report su
www.osservatorio.supercomputing-icsc.it/report/