

Cybersecurity in Italia: sfide e opportunità secondo l'Agenzia per la Cybersicurezza Nazionale (ACN)

Nell'intervento di apertura del 22° Forum ICT Security, Luca Nicoletti – Capo del Servizio Programmi Industriali, Tecnologici e di Ricerca dell'Agenzia per la Cybersicurezza Nazionale (ACN) – ha offerto un'analisi complessiva delle sfide e delle opportunità nel settore della cybersecurity in Italia.

“Come paese e come continente, non possiamo più rimandare la spinta verso l'innovazione” ha dichiarato Nicoletti, enfatizzando l'urgenza di un approccio strutturato e coordinato alla cybersicurezza.

Il suo discorso è stato un richiamo all'azione: richiamando le prime edizioni del Forum e i profondi cambiamenti verificatisi da allora, il rappresentante dell'Agenzia ha evidenziato la necessità di definire risposte condivise tra tutti gli attori coinvolti, sia pubblici che privati.

Cybersecurity in Italia: Trasformazione Digitale e superficie di attacco

Negli ultimi anni la trasformazione digitale ha radicalmente ridefinito il panorama della cybersecurity in Italia.

La crescente interconnessione dei dispositivi e delle reti ha

ampliato la superficie di attacco fino a coinvolgere ogni aspetto della vita quotidiana, dall'IoT domestico alle infrastrutture critiche nazionali: questa espansione richiede un approccio olistico alla sicurezza, che tenga conto anche delle molteplici dipendenze tra i vari sistemi.

Di conseguenza, ciò che vent'anni fa poteva sembrare frutto di una visione futuristica è oggi un pilastro essenziale per garantire la continuità del sistema produttivo e la protezione dei dati personali all'interno di ecosistemi sempre più interconnessi.

In questo contesto, la cybersicurezza è divenuta un elemento imprescindibile per aziende e organizzazioni; la crescita esponenziale della connettività e la crescente adozione di tecnologie avanzate comportano infatti un aumento significativo delle vulnerabilità, rendendo la protezione di sistemi e informazioni una priorità assoluta per qualsiasi Stato.

Evoluzione del quadro normativo europeo

Il quadro normativo europeo è in continua evoluzione per rispondere adeguatamente a queste sfide. Il *Cyber Solidarity Act* rappresenta una pietra miliare nell'ambito della cooperazione transnazionale, introducendo elementi cruciali come i *Rapid Reaction Teams* (RRT).

Nicoletti ha descritto gli RRT come *“unità di reazione rapida che saranno capaci di supportare tutti noi nel ripartire da incidenti”*: integrando competenze in ambito di *threat hunting*, *digital forensics* e *incident response*, questi team rappresentano un significativo passo avanti nella gestione delle crisi informatiche.

Inoltre, il framework normativo introduce protocolli

standardizzati per la condivisione delle informazioni sulle minacce e meccanismi di coordinamento internazionale per la gestione degli incidenti; la capacità di strategie concertate tra i vari Stati membri dell'Unione è fondamentale per garantire una difesa comune che sappia rispondere con efficacia agli attacchi informatici, sempre più spesso caratterizzati da una portata globale.

La Direttiva NIS2 – entrata in vigore il 16 ottobre – costituisce un altro pilastro fondamentale della strategia di sicurezza dell'Unione Europea. La NIS2 stabilisce infatti requisiti tecnici rigorosi per la *security by design*, standard di *reporting* degli incidenti e parametri di resilienza informatica: l'obiettivo è migliorare la sicurezza di sistemi e servizi digitali, promuovendo una gestione proattiva del rischio e una maggiore trasparenza nei processi.

In ossequio alla direttiva, le organizzazioni dovranno implementare misure di sicurezza più stringenti, mostrandosi capaci di rispondere alle minacce informatiche in continua evoluzione.

Questa regolamentazione è essenziale per creare ecosistemi sicuri e resilienti, in grado di sostenere la trasformazione digitale senza comprometterne la sicurezza.

Infrastrutture Strategiche e calcolo ad alte prestazioni

Un progetto strategico su cui l'ACN sta concentrando grandi sforzi è lo sviluppo di un'infrastruttura di calcolo ad alte prestazioni (HPC) a Napoli.

“Con i fondi PNRR stiamo realizzando un importante calcolatore di *high-performance computing*”, ha spiegato Nicoletti; la piattaforma sarà utilizzata per il *machine learning*, l'analisi predittiva delle minacce e la ricerca in campo di crittografia

quantistica e post-quantistica.

L'infrastruttura HPC non solo rafforzerà la capacità tecnologica del paese ma fungerà anche da catalizzatore per la ricerca e l'innovazione, al fine di rendere disponibile una risorsa di calcolo avanzata utilizzabile dall'ACN per rafforzare la sicurezza nazionale, nonché dal mondo accademico e industriale per sviluppare soluzioni all'avanguardia.

Questo progetto rappresenta un esempio concreto di come i fondi pubblici possano essere sfruttati per potenziare le infrastrutture strategiche e supportare la crescita del paese, favorendo lo sviluppo di competenze e la creazione di valore aggiunto in ambito tecnologico e scientifico.



Sfide tecnologiche emergenti: IA e Quantum Computing

Le sfide tecnologiche emergenti, in particolare l'Intelligenza Artificiale e il *computing* quantistico, richiedono una particolare attenzione.

L'Intelligenza Artificiale – ha sottolineato Nicoletti – “è entrata prepotentemente nella nostra vita quotidiana e, come tutte le nuove tecnologie, rappresenta al tempo stesso un'opportunità e un rischio”.

Se infatti l'uso dell'IA nella cybersicurezza rappresenta una frontiera dalle enormi potenzialità, deve essere gestito con grande attenzione per evitare rischi associati all'abuso di queste tecnologie e alle loro possibili implicazioni etiche.

L'ACN sta già lavorando all'implementazione di sistemi di *threat detection* basati sull'IA e allo sviluppo di algoritmi di analisi comportamentale per migliorare la sicurezza nazionale; questi sistemi consentono di rilevare anomalie nei flussi di dati in modo più rapido ed efficiente, rendendo

possibile una risposta tempestiva alle minacce.

Parallelamente, anche il *computing* quantistico rappresenta una sfida senza precedenti.

“Gli algoritmi di crittografia che utilizziamo quotidianamente” ha avvertito Nicoletti *“e tra pochi anni probabilmente saranno obsoleti”*.

Il *computing* quantistico ha quindi il potenziale di compromettere gli attuali metodi crittografici, rendendo vulnerabili i dati sensibili: uno scenario che impone un’urgente transizione verso algoritmi *quantum-resistant* e una revisione completa dei protocolli di sicurezza esistenti, al fine di sviluppare nuovi sistemi di crittografia resistenti ai futuri attacchi quantistici.

La ricerca su questi temi è già in corso, ma richiede investimenti sostanziali e un impegno strategico per garantire che le tecnologie siano pronte prima che il *computing* quantistico diventi una minaccia concreta per la sicurezza informatica.

Investimenti e programmi di sviluppo

Sul fronte dei finanziamenti, l’ACN ha già impegnato **600 milioni di euro dai fondi del Piano Nazionale di Ripresa e Resilienza (PNRR) per lo sviluppo di infrastrutture critiche e il potenziamento delle capacità di *monitoring*.**

Questi investimenti sono destinati sia a rafforzare le infrastrutture esistenti, sia a sviluppare nuove soluzioni per migliorare la resilienza e la sicurezza del paese; sebbene una parte significativa sia vincolata alla digitalizzazione delle Pubbliche Amministrazioni, esistono importanti risorse anche a disposizione delle aziende.

A livello europeo, il Digital Europe Program (DEP) si concentra su progetti con *Technology Readiness Level* (TRL) avanzato, mentre il programma Horizon supporta la ricerca fondamentale e lo sviluppo tecnologico a livello più iniziale: ***“Nei prossimi 2 anni e mezzo ci sono disponibili più di 350 milioni per finanziare programmi di technological uptake”*** ha annunciato Nicoletti, precisando come si tratti di un’importante opportunità per organizzazioni e istituzioni che intendano sviluppare tecnologie avanzate e implementare soluzioni innovative nel campo della cybersecurity in Italia.

L’autonomia tecnologica dell’Europa non è più una priorità rimandabile, perché nessun paese può affrontare da solo le sfide della cybersicurezza moderna: gli investimenti in tecnologie avanzate non rappresentano solo una questione di competitività economica, ma anche di sicurezza nazionale e resilienza strategica.

Resilienza e risposta agli incidenti

In tale quadro l’ACN sta implementando soluzioni all’avanguardia per migliorare la resilienza e la risposta agli incidenti, inclusi *Security Operation Center* (SOC) di nuova generazione e sistemi avanzati di *Security Information and Event Management* (SIEM).

Se i SOC di nuova generazione sono progettati per offrire una visibilità completa sulle reti e rilevare tempestivamente eventuali anomalie che possano indicare un attacco in corso, i sistemi SIEM consentono di aggregare e analizzare una vasta quantità di dati per identificare potenziali minacce e rispondere in maniera efficace.

La cooperazione internazionale rimane essenziale, in particolare rispetto alla condivisione in tempo reale degli Indicatori di Compromissione (IoC) e ai protocolli di risposta

coordinata.

Inoltre, lo sviluppo di tecnologie autoctone e la capacità di gestire autonomamente la sicurezza dei propri sistemi sono aspetti cruciali per garantire la sovranità digitale e la protezione delle infrastrutture critiche, soprattutto a fronte di una situazione geopolitica globale estremamente fluida e imprevedibile.

La creazione di tecnologie avanzate a livello europeo è infatti una priorità assoluta per l'ACN: *“È una cosa che ci chiedono anche i nostri più stretti alleati”* ha evidenziato Nicoletti, ribadendo l'importanza di capacità tecnologiche indipendenti nel contesto dell'UE.

Community Building e Networking internazionale

Infine, Nicoletti ha ricordato che l'ACN sta investendo nel *community building* attraverso piattaforme di condivisione della conoscenza e programmi di certificazione specialistica: *“stiamo costituendo una comunità che sarà agganciata al Centro Europeo di Competenza”*.

La creazione di una solida comunità è infatti essenziale per condividere conoscenze, esperienze e *best practice*, nonché per favorire lo sviluppo di competenze specialistiche in un settore in continua evoluzione.

Evidenziando l'importanza del *networking* internazionale per il futuro della cybersicurezza italiana, il relatore ha concluso con un invito al coinvolgimento attivo delle organizzazioni italiane nella comunità europea, che consentirà di sfruttare al meglio le relative opportunità di finanziamento e cooperazione contribuendo a rafforzare la posizione dell'Italia nel contesto internazionale.

Conclusioni

La visione complessiva dell'ACN sottolinea come la sicurezza informatica richieda un impegno costante nell'aggiornamento

tecnologico e nella ricerca di soluzioni innovative, supportate sia da un framework normativo robusto sia da una cooperazione internazionale costante ed efficace.

Come ricordato da Nicoletti, “il benessere al quale siamo abituati non è scolpito nella pietra, ma è qualcosa che dobbiamo conquistarci tutti i giorni”.

In altre parole la sicurezza informatica non è un risultato statico bensì un processo dinamico e continuo, che richiede l'impegno di tutti gli attori coinvolti: dalla Pubblica Amministrazione alle imprese private, fino al mondo accademico e alla società civile.

Solo attraverso un approccio integrato e collaborativo sarà possibile affrontare efficacemente le sfide della cybersecurity in Italia e garantire un prospero futuro digitale.

Profilo Autore



Luca Nicoletti è nato a Roma nel 1970, si è laureato in Fisica presso l'Università degli Studi di Roma “La Sapienza” nel 1996 con il punteggio di 110/110. Dopo aver svolto il servizio Militare come Ufficiale di Marina, dal 1997 lavora in ambito informatico, interessandosi fin dall'inizio di sistemi distribuiti e tecnologie Web.

I suoi campi di interesse principali sono le Architetture Orientate ai Servizi, virtualizzazione di sistemi e applicazioni, Cloud Computing, sistemi di Identity & Access management, temi sui quali ha prodotto articoli ed è stato chiamato a svolgere seminari.

Tra il 1998 e il 2000 si è occupato di sistemi di Controllo di Gestione per importanti aziende Italiane di Telecomunicazioni ed Energetica. Tra il 2000 ed il 2013 lavora in Consip, prima nell'area “Architetture Tecnologiche” quindi nell'area “System Solution”. Nel 2013 si trasferisce in Sogei S.p.A. nell'area

“Architetture e Servizi Tecnologici” e dal 2018 fino a tutto il 2019 è stato responsabile del gruppo di Demand Management Tecnologico.

Prima In Consip, poi in Sogei, ha inoltre partecipato a numerosi progetti europei nell’ambito del settimo programma quadro (FP7) e del programma Horizon 2020. Dal 2015 al 2018, in rappresentanza del MEF, è stato il Technical Leader del progetto H2020 “Sunfish” e dal 2018 del progetto H2020 “Poseidon”.

Dal 2019 al 2021 ha lavorato in Presidenza del Consiglio dei Ministri, ricoprendo incarichi di responsabile dei servizi IT Dipartimentali e coordinando numerosi gruppi di lavoro, tra i quali quello per la scrittura dei DPCM attuativi del Perimetro di Sicurezza Cibernetica, quello che ha elaborato la componente 5 della Missione 1 del PNRR relativa alla Cybersecurity, quello che ha elaborato la Strategia Cloud Italia e quello relativo alla Strategia Nazionale di Cybersicurezza. Ha partecipato inoltre al gruppo di lavoro che ha elaborato il DL 82/2021 tramite il quale è stata creata l’Agenzia Nazionale per la Cybersicurezza.

Nel corso degli anni ha sviluppato approfondita conoscenze del codice degli appalti pubblici e procedure di gara, nonché nell’esecuzione di contratti complessi.

Attualmente è responsabile del Servizio Programmi Industriali, Tecnologici e di ricerca presso l’Agenzia Nazionale per la Cybersicurezza dove si occupa dell’attuazione della componente Cybersecurity del PNRR e dello sviluppo di nuove capacità industriali e tecnologiche nel settore della sicurezza cibernetica. Con provvedimento a firma del Presidente del Consiglio del 28 febbraio 2022, è stato nominato membro italiano del board del Centro Europeo di Competenza in Cybersecurity (ECCC) di cui al regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/cybersecurity-in-italia/>