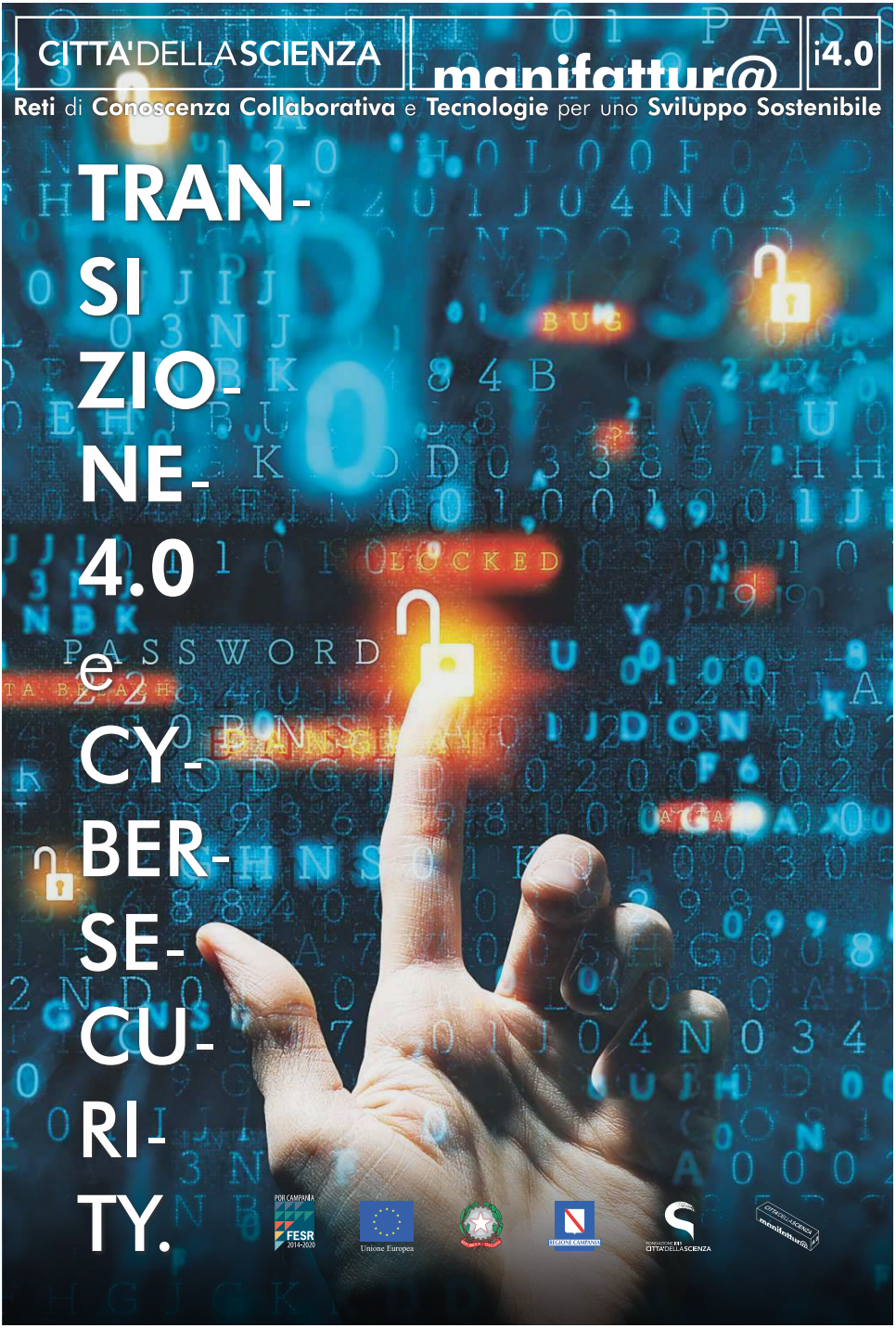
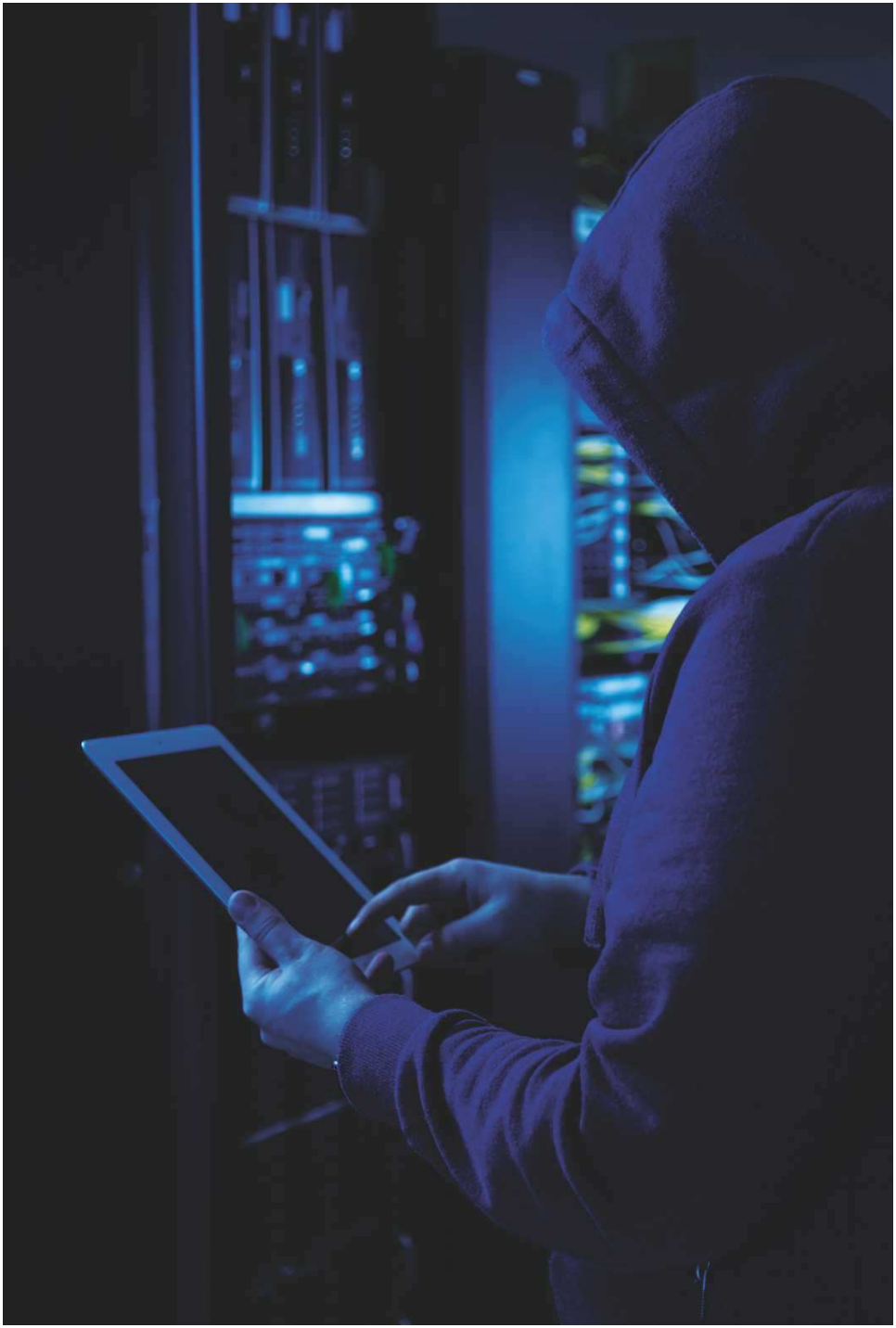
CITTA'DELLASCIENZA
manifattur@
i4.0
Reti di Conoscenza Collaborativa e Tecnologie per uno Sviluppo Sostenibile

TRANSIZIONE 4.0 e CYBERSECURITY.

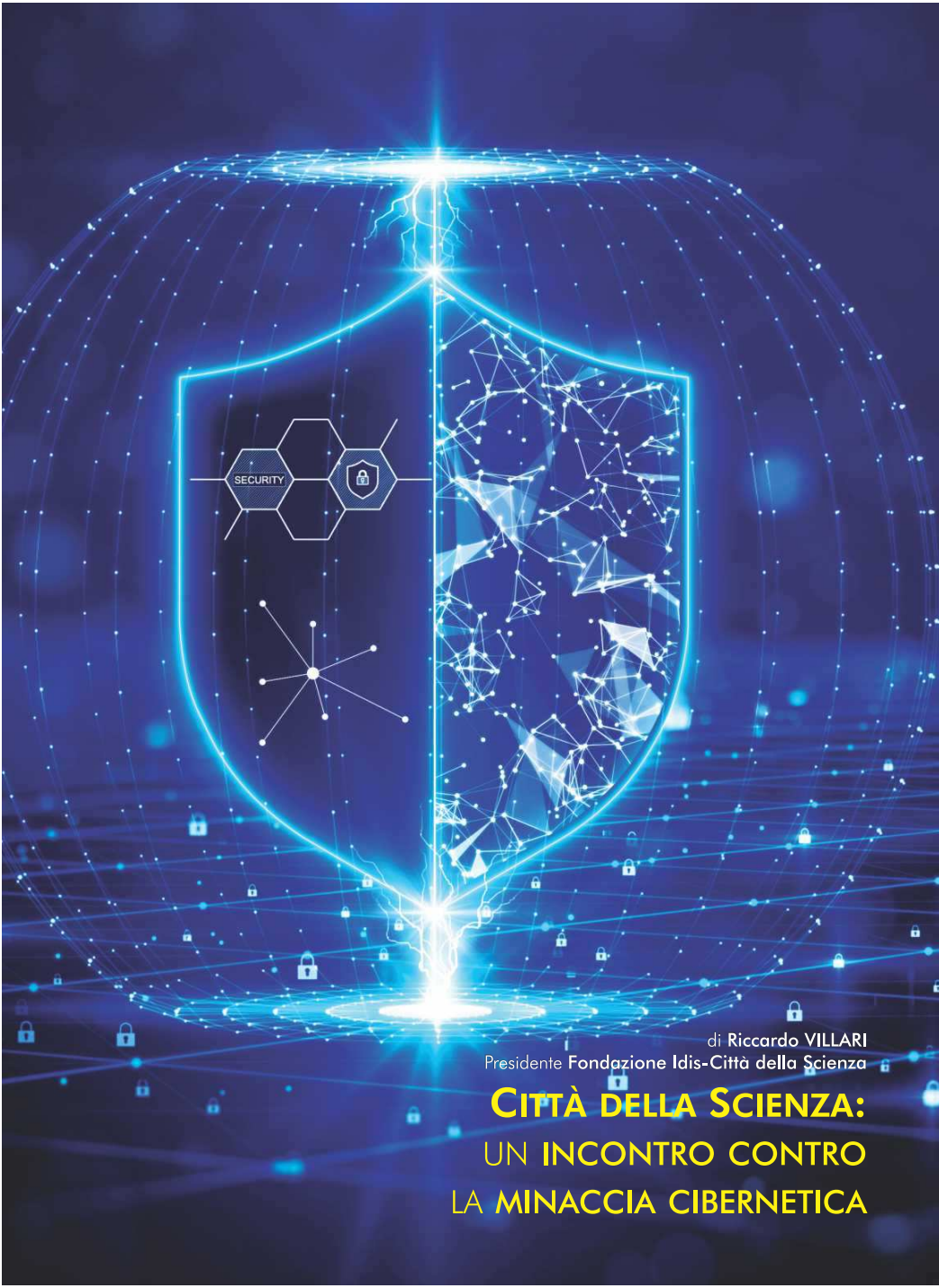


MAGAZINE DIVULGATIVO | N.1 · LUGLIO 2023



INDICE

PROGETTO
STRATEGICO REGIONALE
manifattur@ Campania
industria **4.0**



di **Riccardo VILLARI**
Presidente **Fondazione Idis-Città della Scienza**

CITTÀ DELLA SCIENZA: UN INCONTRO CONTRO LA MINACCIA CIBERNETICA

In un contesto in cui l'influenza sempre maggiore delle nuove tecnologie, la digitalizzazione di tutti i processi, la costituzione di veri e propri patrimoni informativi hanno dato vita a società "sempre connesse", ecco che il tema della *cybersecurity* si fa sempre più attuale. Accanto ai vantaggi, in effetti, appare sempre più evidente la necessità di esporre quelli che sono i rischi che - d'altro canto - insidiano giorno dopo giorno la realtà cibernetica del nostro presente: la *cybersecurity*, infatti, non è altro che l'insieme delle attività di prevenzione, rilevamento e infine neutralizzazione delle minacce che ruotano nel cyberspace, al fine di garantire la protezione dei dati e di tutto quello che può essere esposto a rischi.

Non è un caso, in fondo, che tale discorso attorno alla sicurezza cibernetica abbia trovato espressione proprio alla Città della Scienza di Napoli dove, in occasione del seminario "**TRANSIZIONE 4.0@ CYBERSECURITY: LO SPAZIO DI AZIONE TRA METODI DI VULNERABILITY ASSESSMENT E STRUMENTI PER LA DATA PROTECTION**" tenutosi lo scorso 26 maggio, esperti in materia di Cybersecurity e Transizione 4.0 hanno discusso a lungo sul presente e sul futuro della realtà cibernetica nel nostro Paese dinanzi al continuo aumento di fenomeni di cybercrime.

Città della Scienza, infatti, rappresenta uno dei più grandi poli italiani di diffusione e divulgazione della cultura scientifica che, grazie alle sue attrazione uniche - come Corporea, il Museo Interattivo del Corpo Umano; il Planetario, forse uno dei più belli d'Europa; un polo ricettivo e un incubatore certificato con oltre 40 Start up - registra ogni anno circa 200 mila visitatori, con picchi di anche 2000 presenze al giorno.

Il suo ruolo sul territorio nazionale appare poi particolarmente importante, soprattutto in un contesto odierno in cui la formazione scientifica è fortemente sottostimata. Nel corso dei Saluti di Benvenuto al seminario, è il Presidente della Fondazione Idis-Città della Scienza *Riccardo* **VILLARI** a riconoscere infatti come «oggi se abbiamo carenza dell'intrapresa di percorsi STEM da parte degli studenti, è perché manca quel tipo di orientamento – anche induttivo – che strutture come queste fanno. Immaginate che tutti i musei scientifici, la rete dei musei scientifici in Italia – che è una realtà sconosciuta ai più o sottovalutata – muove circa 2 milioni e mezzo/3 milioni di visitatori: sono numeri da sito di Pompei, quindi veramente c'è tanto da poter lavorare».

I numeri che Città della Scienza raggiunge, d'altronde, sembrano dare ragione a un "investimento culturale" che deve molto al fondamentale sostegno della Regione Campania, che quest'anno ha affidato alla Fondazione la direzione del Progetto Strategico Regionale "**Manifattura Campania: Industria 4.0**", di cui proprio la Cybersecurity rappresenta un nodo importante.

«Il tema della cybersecurity, della sicurezza dei dati», afferma **VILLARI**, «non solo impatta nella vita comune del cittadino, ma anche in quella delle grandi imprese, delle PMI. Insomma, tutti noi viviamo questo problema […]. I numeri sono spaventosi: nell'ultimo anno, la polizia postale ci dice che c'è un aumento di questo problema di oltre il 138 % e l'Italia spende poco - se non sbaglio appena lo 0,10 % del proprio PIL viene destinato ad affrontare questo problema - ma la consapevolezza aumenta e quindi io sono convinto che si saprà anche fronteggiare questa emergenza vera e propria, che in qualche modo impatta nella vita quotidiana di tutti noi».

Il discorso introduttivo del Presidente, dunque, si conclude proprio con la necessità di riconoscere l'importanza del seminario: «Qui al tavolo sono rappresentati tutti gli ambiti che in qualche modo devono trovare una soluzione - analisi e soluzione del problema - che noi cominciamo in maniera corretta ad affrontare, perché appunto connettiamo tutte le varie consapevolezze e le varie competenze affinché si trovi un percorso che bisogna avviare così che questo tema trovi i suoi giusti anticorpi».


#MANIFATTURA #QUARTA RIVOLUZIONE INDUSTRIALE
#TECNOLOGIE 4.0 #INDUSTRIA 4.0 #OPEN INNOVATION
VAI AL
SITO WEB DI
MANIFATTUR@ CAMPANIA: i4.0
A cura dei
referenti della Tecnostruttura di Progetto
"MANIFATTUR@ CAMPANIA:
INDUSTRIA 4.0".
IL SENSO DI UN IMPEGNO
E DI UNA STRATEGIA

In sintonia con il bisogno di salvaguardare e sviluppare le nostre produzioni industriali e manifatturiere, elevandone e qualificandone le capacità produttive in tutte le loro componenti e rendendole **competitive sul piano internazionale, la Regione Campania** è attivamente impegnata a sostenere l'intero sistema socio-economico regionale nel misurarsi al meglio con la sfida della **quarta rivoluzione industriale**.

Le tecnologie 4.0 rappresentano, infatti, non solo i fattori abilitanti per competere al meglio, ma strumenti in grado di trasformare profondamente professioni, amministrazioni pubbliche e abitudini di vita.

Di qui, la necessità di sviluppare un sistema integrato di azioni a regia regionale che, in linea con la L.R. n. 22/2016 "Legge annuale di semplificazione 2016 - **Manifattur@ Campania: Industria 4.0**", la Programmazione Unitaria 2014/2020 e con gli indirizzi della programmazione delle politiche di coesione per il periodo 2021-2027, dimostri di essere in grado di favorire, nel lungo termine, uno sviluppo sostenibile per la Campania fondato sulla diffusione dei processi innovativi tipici del paradigma 4.0. Da un lato, le innovazioni di processo e dell'organizzazione del lavoro, nell'ottica dell'ottimizzazione della produttività, dell'integrazione di filiera, del contenimento dell'impatto ambientale, di migliorie in ambito di sicurezza sul lavoro nonché del coinvolgimento attivo dei lavoratori nel processo produttivo; dall'altro, le innovazioni di prodotto alimentate dallo sviluppo dello spazio cibernetico e delle possibili sue integrazioni con la dimensione reale.

A supporto dei sopramenzionati processi, è fondamentale lo sviluppo di politiche a sostegno dei percorsi di innovazione 4.0 in grado di animare la domanda di innovazione ed esplicitarne i fabbisogni rispetto a cui correlare un'adeguata offerta di servizi di supporto, opportunamente qualificata, potenziata e integrata. Tanto più in presenza di un tessuto produttivo diffuso costituito da piccole e medie imprese che concorrono ad attribuire ai suddetti percorsi la dimensione della transizione 4.0.

Così come critiche risultano essere le azioni tese a promuovere nuove imprese e nuovi mercati, favorendo programmi di *Open Innovation* e potenziando gli spazi da destinare al *co-working* e al *co-design*, nonché le azioni volte all'acquisizione di conoscenze e competenze tali da favorire la capacità di adattamento al cambiamento, così da evitare di subirlo passivamente.

L'insieme di tali aspetti reca in sé la necessità di un'articolata strategia di divulgazione, comunicazione e promozione di contenuti attinenti alle tematiche di sviluppo di Industria 4.0 nonché interventi dimostrativi dei successi tecnologici finalizzati a innalzare il livello di inclusione sociale e raggiungere - in modo istituzionale e partecipato - le periferie dell'ecosistema regionale che diversamente vedrebbero definitivamente compromessa la loro stessa esistenza.

È in questo quadro di azioni che si colloca il Progetto Strategico Regionale "**Manifattur@ Campania: Industria 4.0**", la cui realizzazione, affidata a Città della Scienza, è un momento particolarmente significativo nelle diverse tappe che caratterizzano l'*Industry 4.0 journey* degli attori dell'ecosistema campano. Con tale Progetto si mira, infatti, a creare un *Hub* di densificazione di strumenti, servizi, occasioni di incontro e momenti di co-progettazione che siano di supporto per l'accesso a finanziamenti regionali, nazionali ed europei; alla definizione e realizzazione di percorsi di innovazione; alla progettazione di moduli formativi per lo sviluppo delle nuove competenze; allo sviluppo di nuove imprese in grado di valorizzare i talenti o innescare *partnership* con grandi imprese e PA. Così strutturato, il progetto si configura come strumento essenziale allo sviluppo di percorsi di transizione 4.0 degli attori dell'ecosistema, operando mediante reti di conoscenza collaborativa tra Laboratori universitari, PMI, docenti, studenti e imprenditori, cittadini, istituzioni e Pubbliche Amministrazioni locali.

Una sfida impegnativa della quale questo *magazine* intende essere portavoce, ponendosi come uno dei canali di informazione, approfondimento e continuo aggiornamento sul tema in oggetto. Il primo numero è dedicato al tema della *cybersecurity*, raccogliendo i contributi dei relatori partecipanti al **Seminario** "**Transizione 4.0 @ Cybersecurity**: **lo spazio di azione tra metodi di Vulnerability Assessment e strumenti per la Data Protection**".

A cura di
Antonio **BLASOTTI** e *Martina* **PERILLO**

UNO SPORTELLO PER CRESCERE ED INNOVARE INSIEME NELL'ERA 4.0

VAI ALLA PAGINA WEB
DELLO SPORTELLO
MANIFATTURA 4.0

#MANIFATTURA CAMPANIA #DIGITAL INTENSITY #ECO-SYSTEM #SPORTELLO MANIFATTURA 4.0 #APRE

Il Progetto Strategico Regionale "**Manifattur@ Campania: Industria 4.0**" si pone in capo l'obiettivo di un reale sviluppo delle PMI locali, che trae la propria forza dalle sinergie delle diverse categorie degli stakeholder dell'ecosistema regionale dell'innovazione.
Forte di tale presupposto, il Progetto mira a colmare il *gap* legato alla "*digital intensity*", contribuendo ad allineare la Campania al panorama europeo.

L'evoluzione del progetto è suffragata da momenti di studio e di ricerca con esperti di settore, da una strategia comunicativa volta alla sensibilizzazione e allo sviluppo sia di laboratori, sia di percorsi condivisi di sviluppo di competenze; attivando momenti di confronti *ad hoc* e collaborando con le diverse realtà territoriali, a cominciare dalle Università.

Permettendo alle singole imprese di interpretare il proprio ruolo in un'ottica *eco-system*, il raggiungimento dell'obiettivo passa per l'analisi e la scelta delle traiettorie tecnologiche sulle quali investire per le nuove soluzioni da supportare, e per le modalità di trasferimento di queste ultime dall'offerta alla domanda.

In uno scenario così profilato - e senz'altro in rapido mutamento - la qualificazione di servizi ad alta intensità di conoscenza e l'esplicitazione dei fabbisogni di innovazione, definiti in relazione alle peculiarità dei tessuti produttivi locali, richiedono specifici meccanismi di animazione, promozione, accesso e supporto allo sviluppo/introduzione di soluzioni più o meno mature. Tale processo è un momento necessario per consentire la valorizzazione delle singole tendenze e stemperare i limiti derivanti dalle stesse, altresì necessario per poter valorizzare al meglio le specializzazioni endogene e garantire una prospettiva *glocal* allo sviluppo del sistema regionale, poggiante su una forte tradizione manifatturiera radicata in sistemi di PMI in prevalenza a conduzione familiare, con un saper fare tacito e poco "digitalizzabile".

Per favorire ogni occasione di contatto e di vicinanza al sistema di PMI in evoluzione, è stato realizzato, presso Città della Scienza, lo **Sportello Manifattura 4.0**, che rappresenta un'occasione unica per attivare e gestire gli incontri individuali con gli attori dell'ecosistema legato all'innovazione regionale, interessati a partecipare al progetto e alle altre opportunità in ambito 4.0.

Lo **Sportello Manifattura 4.0** è istituito presso Fondazione Idis-Città della Scienza per pubblicizzare, informare e fornire un primo orientamento agli attori dell'ecosistema dell'innovazione regionale interessati a partecipare al progetto e alle altre opportunità in ambito 4.0. Tali servizi sono qualificati e ampliati grazie alle *partnership* attivate da Città della Scienza con **APRE** (Agenzia Per la Promozione della Ricerca Europea) ed **Invitalia** (Agenzia nazionale per l'attrazione degli investimenti e lo sviluppo d'impresa), che con dei *corner ad hoc* operano presso la sede dello Sportello Manifattura 4.0 a Città della Scienza, n via Coroglio, 57 · Napoli (tel. 081 7352.400 - **email**: sportello@cittadellascienza.it).

Attraverso degli incontri con un consulente, sarà possibile acquisire informazioni sulle opportunità e tematiche legate all'Industria 4.0 per l'elaborazione di attività di analisi, la reingegnerizzazione dei processi e l'innovazione di prodotto e/o di processo, lo sviluppo di piani e progetti preliminari per l'adozione delle tecnologie abilitanti 4.0.

#CYBERSPACE #INTELLIGENZA ARTIFICIALE
#INTERNET OF THINGS #COGNITIVE WARFARE

Elaborazione a cura di
Alessandro **BELLO**, *Fabrizio* **LO REGIO** e *Giuseppe* **NATALINO**

ATTUALI CARATTERIZZAZIONI E CONFIGURAZIONI FUTURE DELLO SPAZIO CIBERNETICO, TRA RICERCA ED INNOVAZIONE

Kuehl, alla fine del primo decennio del XXI secolo, descriveva lo spazio cibernetico come: "Un dominio globale, all'interno dell'ambiente informatico, il cui carattere distintivo e unico è caratterizzato da un uso dell'elettronica e dello spettro elettromagnetico per creare, memorizzare, modificare, scambiare, e sfruttare le informazioni attraverso sistemi interdipendenti e interconnessi che utilizzano le tecnologie delle informazioni e delle comunicazioni" (cfr. D.T. Kuehl, *From Cyberspace to Cyber-power: Defining the Problem, in Cyberpower and National Security*, ed. by F.D. Kramer, S. Starr, L.K. Wentz, National Defense University Press, Washington D.C., 2009).

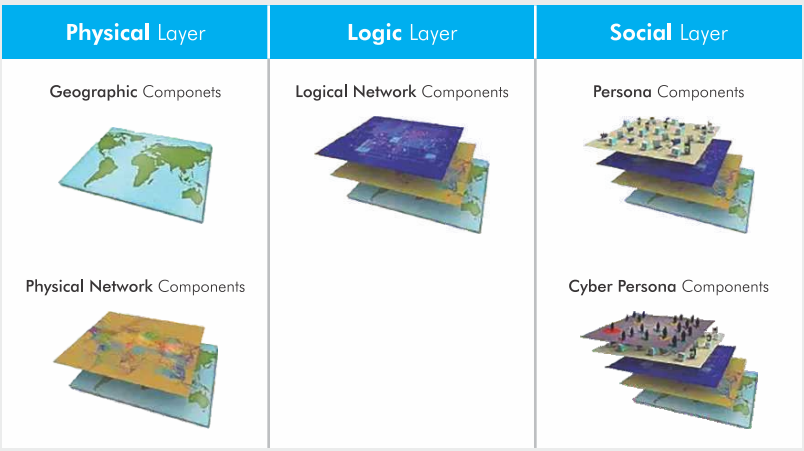
Tra le più recenti rappresentazioni dello spazio cibernetico, vi è quella data dal Dipartimento delle Forze Armate statunitensi, che aggiunge agli elementi tecnici quelli di carattere sociale. Allo **strato fisico** - che include sia la componente geografica (posizione fisica degli elementi della rete), sia quella materiale (*hardware*, infrastruttura, connettori fisici) - e allo **strato logico** - costituito dalle connessioni esistenti tra i nodi di rete - si sovrappone uno **strato sociale**, che comprende gli aspetti umani e cognitivi includendo la componente "*cyberpersona*" (la persona in Rete) e la componente "*user*" (l'utenza in Rete). (cfr. fig. 1)

Nel caratterizzare ampiezza, profondità, estensione e vulnerabilità dello spazio cibernetico è, quindi, necessario considerare il rapporto tra società e tecnologie ICT: due mondi ormai legati indissolubilmente nello spazio cibernetico affermatosi come sostrato tecnologico in cui si estrinsecano le dinamiche politiche, sociali, economico-finanziarie e umane.

«Internet si è trasformato e nella trasformazione di Internet si è trasformato il mondo», così ha esordito con il suo intervento il prof. *Vincenzo* **LOIA**, Magnifico Rettore dell'Università di Salerno e Presidente della Fondazione SERICS - *SEcurity and RIghts In the CyberSpace*, che riunisce i principali Centri di ricerca e importanti imprese interessate allo sviluppo della ricerca in ambito della sicurezza informatica in Italia.

«Oltre 5 miliardi di persone (ossia circa il 65% della popolazione globale) hanno oggi accesso a Internet stabilendo, al di là delle frontiere geografiche, scambi di informazioni, condivisione di conoscenza e transazioni di prodotti reali e/o digitali con moneta reale e/o virtuale a livello globale», ha affermato il Magnifico Rettore dell'Università di Salerno.
«Attraverso lo spazio cibernetico si realizzano sempre più le fondamentali libertà di informazione, di espressione e di associazione del cittadino (l'utente medio globale di Internet trascorre sette ore *online* ogni giorno, mentre *Google* elabora 8,5 miliardi di *query* di ricerca ogni giorno in tutto il mondo) in nuovi contesti di azione in cui il *mobile*, l'Intelligenza Artificiale e l'*Internet of Things* ridefiniscono ruoli, tempistiche e spazio di azione (a partire da novembre 2022, i dispositivi mobili hanno generato il 59.6% del traffico globale dei siti web; nella prima metà del 2022, il 42% di tutto il traffico Internet era automatizzato, di questo oltre il 50% attraverso *bot* cattivi, il 75% delle persone non scorre mai oltre la prima pagina dei risultati di ricerca e tra il 70 e l'80% ignora *Google* annunci)».

Figura 1 - Possibile stratificazione dello spazio cibernetico



Fonte: Department of the Army Headquarters, United States Army

Lo stesso scenario internazionale, sotto la spinta propulsiva della "democratizzazione delle informazioni", sta radicalmente evolvendosi da unipolare verso una architettura pressoché multipolare, con nuovi attori capaci di influenzare e modellare i processi decisionali delle comunità digitali assumendo, non di rado, comportamenti opportunistici, fino alla dimensione terroristica, grazie al significativo abbassamento della soglia di accesso alla "violenza", effetto combinato dell'economicità degli strumenti informatici e del relativo anonimato. Il dominio cibernetico è diventato, ben presto, vettore nonché potenziale "moltiplicatore" delle minacce per la sicurezza.

Se da un lato lo sviluppo dei dispositivi, che dialogano tra loro e con gli operatori e la crescente interconnessione - interoperabilità delle infrastrutture fisiche digitalizzate (come ad esempio acquedotti, reti di trasporto civile e reti energetiche, o ancora i sistemi di comando e controllo militari, le applicazioni domotiche e i sistemi di guida autonoma e commessa, i *cobot* e i *surgical robot*) - rendono l'intero spazio cibernetico maggiormente *smart* ed efficiente; dall'altro, ne sanciscono una diffusa vulnerabilità ed una maggiore esposizione. Ciò pone una sfida complessa per chi ha il compito di tutelare e proteggere i contesti di interazione digitale, affinché possano essere aperti, affidabili e sicuri.

Invero, la crescente dipendenza delle società moderne dallo spazio cibernetico rende sempre più grave il danno che può giungere dalla compromissione delle reti o da mirati attacchi attraverso di esse. Tanto più che le minacce possono originare da qualsiasi punto della rete globale e, spesso, colpiscono gli anelli più deboli della catena, ossia i soggetti più fragili o i sistemi meno protetti.

L'interdipendenza delle reti e la pervasività dello spazio cibernetico con l'asimmetricità della minaccia impongono di sviluppare un approccio olistico per poter assicurare un accettabile livello di sicurezza cibernetica. «Il rischio del *cyber* terrorismo è globale e gli attacchi sono rapidi», ha commentato il prof. **LOIA**, «[…] appare fondamentale instaurare delle collaborazioni tra aziende, centri universitari ed enti governativi nazionali e sovrannazionali per potenziare a livello sistemico le capacità di prevedere e prevenire un attacco, per individuarlo nel momento in cui accade, per reagire ad esso e mitigarne gli effetti, per risalire ai responsabili, oltre che per ristabilire rapidamente la funzionalità originaria».

Il campo di battaglia si sta allargando ricomprendendo il *layer* sociale (cfr. fig. 1), con azioni tese a manipolare la comprensione e minare la capacità degli utenti di conoscere e di giudicare (*Cognitive Warfare*); ne sono esempi: il dirompente uso di *fake news*, protagoniste degli ultimi eventi d'interesse globale, come la pandemia da Covid-19 e l'invasione russa dell'Ucraina.

In tali casi, agli elementi tipici di vulnerabilità dello spazio cibernetico (infrastruttura e logica delle reti) si aggiungono dimensioni sociali quali l'analfabetismo digitale, l'eccesso di fiducia, la conferma di pregiudizio, l'isolamento sociale, la limitata diversità delle fonti, la bassa capacità di giudizio critico, la frustrazione e la rabbia dell'utente.

Sicché «il rischio che in Italia la rete possa essere inondata da credibili falsificazioni non è da sottovalutare, considerato che un terzo degli italiani è considerato funzionalmente analfabeta nell'ambito digitale, questo fenomeno dev'essere combattuto educando le persone a comprendere e interpretare correttamente le informazioni che ascoltano in TV o leggono sulle testate *online*».

La tecnologia, da sola, non è quindi sufficiente per affrontare le sfide della sicurezza informatica: è infatti fondamentale un approccio che coinvolga la consapevolezza, la collaborazione e l'educazione di tutti. Il Rettore conclude affermando che il primo passo di questo processo è rivolgersi ai giovani, cercando di indicargli la giusta strada per capire come reagire ai fenomeni che li coinvolgono *online*, come il *cyberbullismo*.

[**L'articolo è tratto** dall'intervento del prof. *Vincenzo* **LOIA** tenuto nel corso del seminario "Transizione 4.0 @ Cybersecurity"]

Prof. *Vincenzo* **LOIA**,
Magnifico Rettore - Università di Salerno
e Presidente della Fondazione SERICS
Security and Rights in the CyberSpace

RIVEDI IL SUO INTERVENTO

Elaborazione a cura di
Armando **CARCATERRA** e *Maurizio* **DI MEGLIO**

I SERVIZI AVANZATI IN AMBITO CYBERSECURITY DELLA $R^2Lab_{4.0}$

La formalizzazione e il potenziamento della $R^2Lab_{4.0}$ - Rete Regionale dei Laboratori 4.0 sono tra i principali obiettivi del Progetto Strategico Regionale "**Manifattur@ Campania: Industria 4.0**" (da ora Progetto M4.0).

Affidato per la relativa attuazione a Fondazione Idis-Città della Scienza, il Progetto è finanziato dalla Regione Campania nell'ambito del PO FESR 2014-2020, con l'obiettivo di dare impulso alla **transizione 4.0** dell'ecosistema regionale campano, contribuire a colmarne il *gap* di "*digital intensity*" e valorizzare l'impiego di competenze e produzioni locali. Un tale percorso, in coerenza con le logiche a base della *smart specialization*, richiede la necessità di scegliere su quali tecnologie abilitanti investire, come trasferirle dall'offerta alla domanda, come valorizzarle nel momento implementativo e come integrarle a livello organizzativo per cogliere al meglio le molte opportunità offerte dai percorsi di innovazione implementabili.

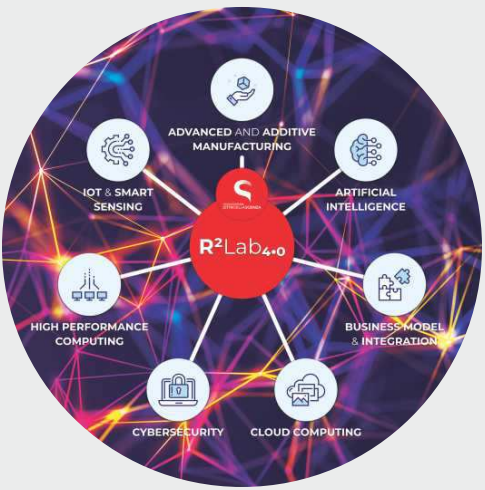
Di qui, la previsione, all'interno del Progetto M4.0, dell'azione "**2.1 - Attivazione e qualificazione dell'offerta di servizi di supporto in ambito I4.0**" che, opportunamente integrata con gli *Audit* dei fabbisogni tecnologici per la transazione 4.0 delle PMI e una preliminare mappatura dei provider dei servizi e tecnologie 4.0, ha come principale obiettivo la formalizzazione della $R^2Lab_{4.0}$ e il potenziamento infrastrutturale dei relativi nodi.

La *mission* della costituenda rete è quella di rendere disponibile alle PMI manifatturiere campane e alle PA locali, il patrimonio di competenze qualificate e di infrastrutture di R&S e di Innovazione (laboratori, impianti e strumentazioni) regionali, messi a sistema dalla stessa Fondazione Idis-Città della Scienza, in qualità di *HUB* di coordinamento della rete, con il coinvolgimento delle Università pubbliche della Campania.

Ad oggi, a valle della partecipazione di un'apposita manifestazione di interesse e di uno strutturato processo di selezione, i soggetti fondatori della rete sono l'Università di Napoli Federico II e l'Università degli Studi di Salerno. La prima, impegnata a gestire il nodo *Artificial Intelligence*, il nodo *High Performance Computing* e il nodo *IoT & Smart Sensing*; i nodi di interesse dell'Università di Salerno sono, invece, relativi alle aree tecnologiche prioritarie della *Cybersecurity*, del *Cloud Computing*, e del *Business Model & Integration*. Completa la rete il nodo dedicato alle tecnologie per l'*Advanced and Additive Manufacturing* di competenza del D.re.a.m. Fab Lab di Fondazione Idis-Città della Scienza.

Al fine di sfruttare le complementarità e i vantaggi di un'adeguata massa critica di risorse strumentali e competenze tecniche distribuite e diffuse sul territorio regionale, la partecipazione alla rete è aperta (mediante richiesta di accreditamento).

I servizi ad oggi disponibili presso i sette nodi della rete sono stati scelti mediante un processo di *fine tuning* dell'offerta, che è partito dai risultati di un'attività di *audit* per intercettare i fabbisogni tecnologici delle PMI nel contesto regionale, e ha permesso di valorizzare, con investimenti in attrezzature e *facilities innovative*, le competenze e il *know-how* dei Dipartimenti delle Università partecipanti. Per ciascuna tipologia di servizio è stato definito l'ambito di applicazione, il *target* (di aziende e PA) a cui si rivolgono, l'*output* atteso, le competenze minime richieste all'acquirente per la relativa implementazione e una base di prezzo per l'accesso al servizio.



In particolare, i servizi che vengono offerti nell'ambito della *Cybersecurity* sono cinque e sono stati dettagliati dal prof. *Alfredo* **DE SANTIS**, Ordinario di Informatica presso il Dipartimento di Informatica dell'Università di Salerno e Responsabile del Nodo *Cybersecurity* della **R^{2}Lab**$_{4.0}$. «Si tratta, essenzialmente, di servizi del tipo *off the shelf* (pronti all'uso)», afferma il prof. **DE SANTIS**, «che, quindi, possono essere utilizzati dalle varie aziende senza dover modificare la loro struttura organizzativa e senza mettere a disposizione ulteriori risorse proprie».

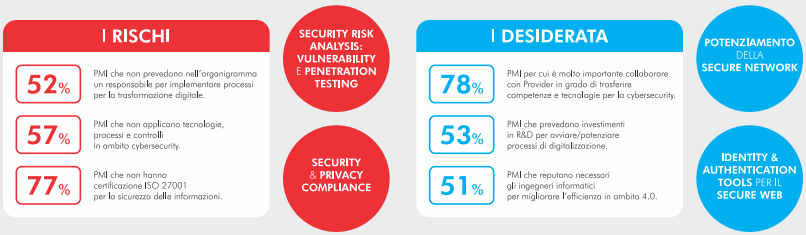
Inoltre, scorrendo i cinque servizi, la logica utilizzata per la strutturazione del sistema di offerta del nodo rende i servizi iniziali elemento di accesso per quelli successivi fino all'utilizzo della *Blockchain*.

Tutto ciò è in coerenza con le risultanze di indagini *ad hoc* svolte da Fondazione Idis-Città della Scienza, «che hanno visto la partecipazione effettiva di oltre 100 PMI intervistate, le quali hanno permesso di avere un primo quadro del livello di interesse dei singoli servizi del nodo *Cybersecurity* ed affinare il processo di relativa specificazione».

La riscontrata adeguatezza dei servizi rispetto ai desiderata delle PMI permetterà al nodo *Cybersecurity* della **R^{2}Lab**$_{4.0}$, inoltre, di implementare in modo spedito a seconda fase di qualificazione dell'offerta di servizi di supporto in ambito I4.0, con la realizzazione - in collaborazione con le PMI - di progetti pilota finalizzati a dimostrare l'effettiva capacità del nodo di soddisfare le esigenze di innovazione 4.0.

[**L'articolo è tratto** dall'intervento del prof. *Alfredo* **DE SANTIS** tenuto nel corso del seminario "Transizione 4.0 @ Cybersecurity"]

SERVIZIO	AMBITO APPLICATIVO
CYBSEC.1 · SECURITY RISK ANALYSIS: VULNERABILITY ASSESSMENT E PENETRATION TESTING	• Identificare la superficie di attacco, i punti deboli e le eventuali vulnerabilità IT di un'organizzazione (strumentazioni IT, applicazioni web, infrastruttura di rete); • Vulnerability Assessment, per l'identificazione di vulnerabilità comuni; • Penetration Test per identificare vulnerabilità non comuni.
CYBSEC.2 · SECURITY & PRIVACY COMPLIANCE	• Analizzare il livello di adeguatezza e definire percorsi per assicurare il raggiungimento/mantenimento di un'effettiva compliance normativa rispetto ai requisiti di sicurezza e privacy delle principali legislazioni e/o standard.
CYBSEC.3 · POTENZIAMENTO DELLA SECURE NETWORK	• Analisi dell'architettura di una rete aziendale esistente e identificazione delle possibili problematiche di sicurezza; • Definizione di un possibile piano di evoluzione della rete al fine di superarne le criticità e di alzare i livelli di sicurezza.
CYBSEC.4 · IDENTITY & AUTHENTICATION TOOLS PER IL SECURE WEB	• Sviluppo di un microservizio che mira a definire delle soluzioni IAM in contesti centralizzati e decentralizzati basandosi sui principali standard OpenIDConnect, Fido2 e altri, impiegando database centralizzati e/o blockchain.
CYBSEC.5 · ARCHIVIAZIONE E NOTARIZZAZIONE MEDIANTE TECNOLOGIA BLOCKCHAIN	• Sviluppo di una soluzione a microservizio per la gestione di documenti digitali; • Gestione e archiviazione sicura di documenti digitali con valore legale; • Sensibilizzazione verso l'utilizzo di applicazioni decentralizzate basate su blockchain e la loro notarizzazione su tecnologia blockchain.



[1] Il processo di selezione dei soggetti gestori dei nodi della $R^2Lab_{4.0}$ e il processo di potenziamento infrastrutturale e qualificazione ha visto le seguenti fasi: A) Analisi del contesto tecnologico da parte di Fondazione Idis; B) Presentazione dei Piani di potenziamento dei Laboratori di Ricerca 4.da pate del CESMA di UNINA e DI & DISAMIS di UNISA a valle di una Manifestazione di Interesse; C) Valutazione dei Piani da parte del CTS di Fondazione Idis-Città della Scienza; D) Negoziazione e approvazione dei Piani esecutivi (fase opportunamente informata dai risultati in itinere dell'audit dei fabbisogni tecnologici per la transizione 4.0 delle PMI Campane sviluppata da CdS). Ciò ha portato alla formalizzazione di una prima struttura della Rete e ad un primo Catalogo dei servizi 4.0, che saranno opportunamente ampliati nel corso del progetto per effetto dell'attesa partecipazione di ulteriori soggetti qualificati alla rete stessa.

[2] Presso il sito web **https://manifattura4puntozero.cittadellascienza.it/** alla sezione partecipata è possibile compilare il questionario "MAPPATURA DEI PROVIDER DEI SERVIZI A SUPPORTO DELLA TRANSIZIONE 4.0" con cui è possibile candidare i propri servizi alla Rete.

[3] L'indagine svolta da CdS, che ha coinvolto oltre 500 aziende tra PMI, PMI Innovative e Start up Innovative, ha raccolto la partecipazione attiva di oltre 100 imprese che, opportunamente supportate, hanno permesso di avere una prima rappresentazione puntuale degli interessi all'innovazione in materia di *cybersecurity* del sistema delle imprese campane, ciò ha permesso, in sede di negoziazione dei Piani, di raffinare e meglio correlare i servizi del nodo.

Prof. *Alfredo* **DE SANTIS**,
Professore Ordinario di Informatica
presso il Dipartimento di Informatica dell'Università
degli Studi di Salerno e Referente del Nodo
Cybersecurity della R2Lab4.0

RIVEDI IL SUO INTERVENTO

#CYBERSECURITY #RAPPORTO CLUSIT
#MANUFACTURING #RISK ASSESSMENT

Elaborazione a cura di
Stefano **DE LISE** e *Andrea* **ESPOSITO**

CYBERSECURITY NEL SETTORE MANIFATTURIERO, FRA EVOLUZIONE DEGLI SCENARI DI RISCHIO E REQUISITI NORMATIVI

Il 2022 si caratterizza come l'anno peggiore da sempre per la *Cybersecurity*. Confrontando i numeri del 2018 con quelli del 2022 la crescita del numero di incidenti gravi a livello globale è stata del 60% (da 1.554 a 2.489), con 440 in più rispetto al 2021 (+21%).

Nel contesto delle crescenti tensioni internazionali tra superpotenze e di un conflitto ad alta intensità combattuto ai confini dell'Europa, anche l'Italia appare ormai in maniera evidente nel mirino: nel 2022 nel nostro Paese, con 188 attacchi portati (+169% rispetto all'anno precedente), è andato a segno il 7,6% degli attacchi globali (contro il 3,4% del 2021). A completare il quadro italiano, la gravità elevata o critica nell'83% dei casi.

Nonostante la natura più complessa degli attacchi, il 64% degli incidenti a livello globale hanno come causa azioni "maldestre" degli utenti o del personale informatico nelle aziende. Infatti, rispetto al totale degli attacchi, i *malware* (per il 37%), la vulnerabilità (per il 12%), il *phishing*, il *social engineering* e l'*account cracking* (per il 12%), sono le tecniche principali di aggressione utilizzate, segnando nel complesso un incremento complessivo del 52% sul totale rispetto allo scorso anno.

Sono questi i dati che emergono dal **Rapporto 2023 della Clusit**, Associazione Italiana per la Sicurezza Informatica che, con la *mission* di promuovere e diffondere nel nostro paese la cultura e la consapevolezza della sicurezza informatica in tutti i suoi aspetti, conta tra i suoi soci alcune delle principali aziende IT, centri di ricerca e imprese manifatturiere e di *utilities* italiane.

Dall'ultimo Rapporto Clusit, emerge inequivocabilmente come l'accelerazione nella digitalizzazione dei processi di *business* e la conseguente virtualizzazione delle interazioni sociali ed economiche, anche correlati alla diffusione del lavoro da remoto, le crescenti dipendenze dalle filiere di approvvigionamento (*supply chain*), abbiano contribuito ad incrementare la superficie di esposizione sfruttabile per la conduzione di attacchi *cyber* efficaci ai danni di cittadini, organizzazioni e istituzioni. «Man mano che le risorse di valore si spostano sul digitale, anche la parte più delinquenziale si sposta in quella direzione», ha affermato *Claudio* **TELMON**, Consulente e *Adviser* nel campo della sicurezza e dell'audit ICT, nonchè membro del Comitato Direttivo della CLUSIT.

È il caso del *Manufacturing*, che ha fatto registrare un aumento costante dal 2% del 2018 al 5% del 2022, per effetto della sempre maggiore diffusione dell'IoT e dalla tendenza verso l'interconnessione dei sistemi industriali che, come è (purtroppo) noto, risultano molto spesso non sufficientemente protetti, diventando un punto di accesso facile per gli attaccanti.

Ciò, secondo **TELMON**, «è dovuto alla scarsa attenzione alle tematiche legate alla sicurezza informatica, spesso collegata ad una sottostima della preziosità dei dati e alla conseguente ridotta percezione dell'effettivo rischio di subire attacchi sui medesimi».

Sicché tra i soggetti importanti da monitorare per assicurare la resilienza in materia di sicurezza informatica, sono state incluse - con la recente pubblicazione della nuova direttiva NIS2 [DIRETTIVA (UE) 2022/2555] - le imprese manifatturiere operanti in specifici comparti critici per l'economia degli stati membri (es. fabbricazione di prodotti chimici, di dispositivi medici e medico-diagnostici, di computer e prodotti elettronici e ottici, di apparecchiature elettriche, della fabbricazione di macchinari e apparecchiature n.c.a., della fabbricazione di autoveicoli, rimorchi e semirimorchi, della fabbricazione di altri specifici mezzi di trasporto, dei servizi digitali e della ricerca). Le imprese operanti in tali settori sono oggi chiamate ad implementare un adeguato processo di *risk assessment* per la gestione degli eventi *cyber* potenzialmente malevoli, sia interni (manutenzione dei sistemi informatici e di rete, gestione degli incidenti e della continuità operativa), che esterni (es. verso i propri fornitori).

◂ Dott. *Claudio* **TELMON**, Consulente e Adviser nel campo della sicurezza e dell'audit ICT e membro del Comitato Direttivo della CLUSIT

RIVEDI IL SUO INTERVENTO

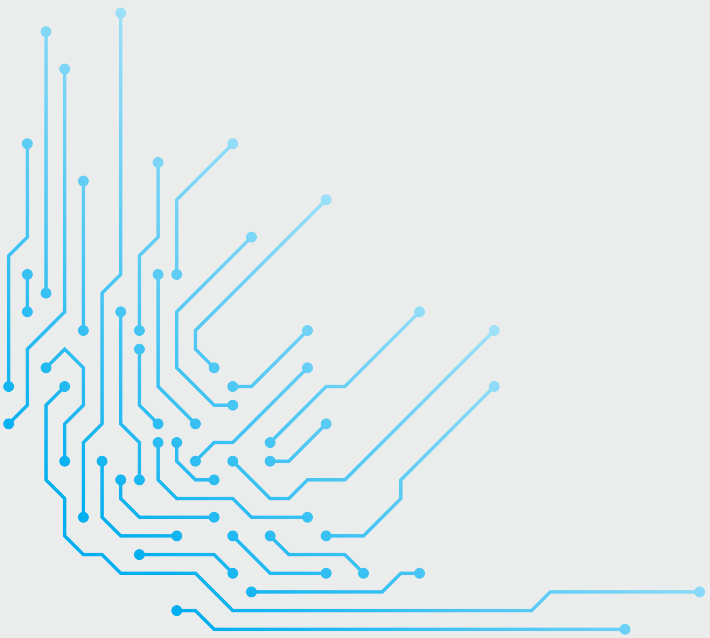
«Gli obblighi normativi, che hanno lo scopo di assicurare la capacità di garantire l'offerta sicura di servizi e prodotti alla collettività, non sono da considerare vessatori... purché», ha tenuto a sottolineare **TELMON** «le aziende sappiano fare sistema per sopperire alla carenza di competenze in materia di *cybersecurity* e si convincano ad adottare *framework* riconosciuti, al fine di rispondere alle richieste normative e della *supply chain*».

Inoltre, è importante sensibilizzare i vertici aziendali e la proprietà in merito all'importanza della cybersicurezza, evitando così di dover interrompere i processi produttivi a causa di attacchi informatici. A tal proposito, la NIS2 prevede che vengano definite responsabilità molto precise in capo agli organi di gestione delle organizzazioni.

Infine, è particolarmente importante monitorare e poi pianificare in vista degli incidenti, al fine di limitare i danni.

In conclusione, la sicurezza informatica rappresenta una sfida quotidiana per le aziende di tutti i settori e un vero e proprio problema per la collettività. Per tale motivo, è necessario porre in essere tutte quelle azioni in grado di tutelare la comunità nel complesso.

[**L'articolo è tratto** dall'intervento del dott. *Claudio* **TELMON** tenuto nel corso del seminario "Transizione 4.0 @ Cybersecurity"]



Elaborazione a cura di
Roberta **AURELIO** ed *Emanuela* **CACCIATORE**

IL **RUOLO** DEGLI **OPERATORI TELCO** NEL **MERCATO** DELLA **CYBERSECURITY**

La *Cybersecurity* è un problema trasversale che riguarda tutto il sistema Paese e che colpisce indifferentemente individui e organizzazioni di ogni genere.

Uno scenario non positivo con un forte *trend* in crescita per la sicurezza delle informazioni e dei dati, in cui è necessario sviluppare piani adeguati e risolutivi per prevenire e gestire gli accessi non autorizzati. Ne consegue che è necessario conoscere le persone, i processi e le tecnologie per proteggersi con misure preventive, conoscere i propri utenti e sistemi, le vulnerabilità e le minacce per rilevare eventuali attacchi, rispondere in modo tempestivo ed efficace per ripristinare la piena operatività.

Il dott. *Claudio* **MANTOVANI**, Responsabile del *Competence Center Enterprise* presso Fastweb, esperto nel campo della sicurezza informatica e della protezione delle infrastrutture all'interno di Fastweb, è intervenuto nel corso del seminario sulla "Transizione 4.0 @ *Cybersecurity*: lo spazio di azione tra metodi di *Vulnerability Assessment* e strumenti per la *Data Protection*", lo scorso 26 maggio presso la Sala Archimede della Città della Scienza di Napoli, fornendo un'importante testimonianza aziendale in merito alle principali criticità e rischi informatici in ambito *cybersecurity*.

In riferimento al rapporto Clusit 2022 - il *report* sulla sicurezza ICT dell'Associazione Italiana per la Sicurezza Informatica - l'analisi Fastweb evidenzia un aumento degli attacchi *cyber* del 25%, pari cioè a 56 milioni. Diminuisce, tuttavia, del 9% la quantità di *server* e *device* a rischio. All'avanzare degli attacchi informatici, infatti, si contrappone una sempre maggiore efficacia delle misure di difesa, grazie anche ad una progressiva consapevolezza rispetto ai rischi informatici da parte delle aziende e delle pubbliche amministrazioni, che indirizzano maggiori investimenti verso tecnologie e servizi nell'area *Security*.

MANTOVANI ha sottolineato che «l'attuale complessità della lotta contro gli attacchi informatici è frutto di uno scenario sbilanciato in cui gli aggressori possono sfruttare distrazioni, vulnerabilità o errori di configurazione di soggetti poco "interessanti" per compromettere i sistemi di attori critici».

Il "difensore" si trova a dover gestire infrastrutture sempre più complesse ed integrate con quelle di altri attori, quindi soggette ad una superficie di attacco non sempre integralmente monitorata.
«Dire che sono aumentati gli attacchi, vuol dire che abbiamo avuto delle importanti polarizzazioni di fenomeni sul mercato italiano di nuove tipologie di attacco che si sono sommate a quelle che già esistevano», spiega il relatore.

Nel corso del 2022, Fastweb ha raccolto dati da una posizione privilegiata sulla rete, permettendo di osservare gli attacchi informatici in Italia. Si è notato un aumento delle aggressioni opportunistiche e mirate. Gli attacchi opportunistici colpiscono le organizzazioni meno preparate, mentre quelli mirati hanno obiettivi specifici come i settori finanziari e le amministrazioni pubbliche.
La complessità degli scenari e delle tecniche di attacco è aumentata, specialmente con l'utilizzo di Intelligenza Artificiale e tecniche di *phishing* sofisticate.

◂ Dott. *Claudio* **MANTOVANI**,
Responsabile del Competence Center
Enterprise presso Fastweb

RIVEDI IL SUO INTERVENTO

Tutto ciò richiede, secondo il Responsabile del *Competence Center Enterprise* presso Fastweb, una gestione integrale della *cybersecurity* in grado di contemperare sei **punti chiave** su cui focalizzarsi per garantire la sicurezza aziendale:

- integrazione delle infrastrutture (conoscere i sistemi informatici presenti in azienda);
- azioni di *risk assessment* e *compliance* per valutare il livello di rischio;
- creazione di sistemi specifici per la visibilità e la protezione;
- gestione delle vulnerabilità e delle minacce potenziali;
- iniziative di *assessment* e formazione per aumentare la consapevolezza e le competenze che servono in tutta l'azienda già in fase preliminare;
- attività di monitoraggio automatizzato basato sull'intelligenza artificiale.

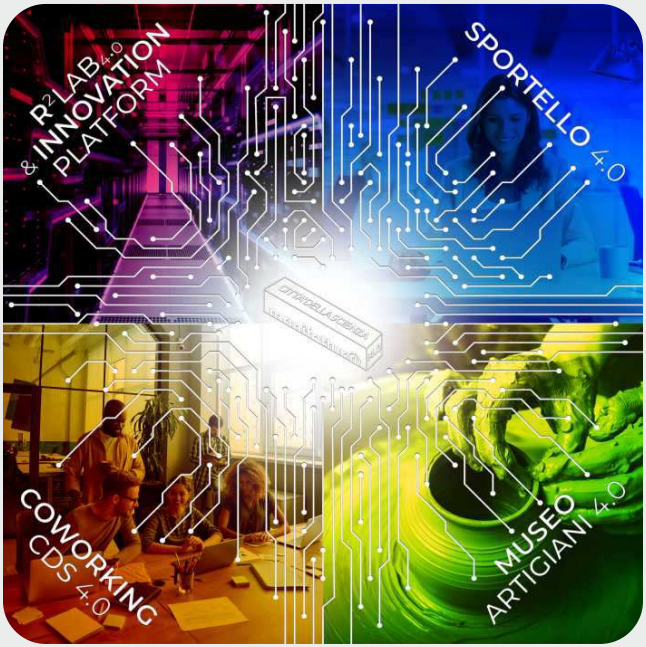
La digitalizzazione ha ampliato il perimetro di sicurezza, coinvolgendo infrastrutture *on-premises*, *cloud* pubblici e terze parti. È fondamentale, dunque, mantenere una gestione coerente e garantire la sicurezza in tutti questi ambienti.

In termini di innovazione, è importante - sottolinea **MANTOVANI** - la necessità di integrare la sicurezza nella progettazione dei prodotti e dei servizi, adottando il concetto di *security by design*, che non deve essere considerato un valore aggiunto, piuttosto uno *standard* a cui tendere.

«È necessario considerare la sicurezza sin dalle fasi iniziali, poiché correggere eventuali difetti in seguito può risultare molto oneroso e complesso in termini di *budget*, ma anche per gestire gli attacchi informatici in modo tempestivo ed efficace con un processo solido di gestione degli incidenti».

[**L'articolo è tratto** dall'intervento del dott. *Claudio* **MANTOVANI** tenuto nel corso del seminario "Transizione 4.0 @ Cybersecurity"]

GESTIONE EFFICACE DELLA **CYBERSECURITY:** ASPETTI CHIAVE



Ringraziamo per le testimonianze:

Ing. *Giovanni Maria* **D'ANTONIO**,
Responsabile dell'Information Security Management System, sito STMicroelectronics di Marcianise. STMicroelectronics è uno dei più grandi produttori mondiali di componenti elettronici, usati soprattutto nell'elettronica di consumo, nell'automotive, nelle periferiche per computer, nella telefonia e nel settore cosiddetto "industriale".

Ing. *Giovanni* **SALATIELLO**,
Responsabile tecnico della NETcaring srl. NETcaring è una società di consulenza IT che progetta infrastrutture IT e sviluppa soluzioni software custom di classe Enterprise & Real-Time nei vari campi applicativi: Network, Enterprise e Technology.

#PUBBLICA AMMINISTRAZIONE #SERVIZI DIGITALI
#TRANSIZIONE DIGITALE #DISASTER RECOVERY
#SECURITY OPERATION CENTER #DIGITAL TWIN

Elaborazione a cura di
Carmen **FABIANO** e *Aldo* **ARPAIA**

LE **MISURE** DI **POTENZIAMENTO** DELLA **SICUREZZA** DEI **SERVIZI PUBBLICI DIGITALI** IMPLEMENTATE IN **REGIONE CAMPANIA** E GLI **INTERVENTI** DEL **PR FESR 2021-2027** IN **MATERIA** DI **DIGITALIZZAZIONE**

I processi di trasformazione digitale - che stanno cambiando il volto e il rapporto della Pubblica Amministrazione nei confronti dei cittadini e delle imprese, permettendo l'accesso ad un'offerta di servizi sempre più efficienti e facilmente accessibili - richiedono di agire su due dimensioni.

Da un lato, per garantire la normale operatività della Pubblica Amministrazione, è necessario rendere più robusti gli *asset* dell'infrastruttura digitale, più solide le capacità tecniche di valutazione e più presenti *audit* della sicurezza di apparati elettronici, reti e applicazioni utilizzati per l'erogazione dei servizi. Dall'altro, per consolidare il rapporto di fiducia con i cittadini, è opportuno adottare soluzioni in grado di ridurre il livello di vulnerabilità da minacce *cyber* su tutti i fronti (es. frodi, ricatti informatici o attacchi terroristici) rafforzando la capacità dei presidi di *front-line* per la gestione degli *alert* e degli eventi a rischio.

In Regione Campania, è l'Ufficio Speciale per la crescita e la Transizione Digitale, istituito nel 2021 e diretto dal dott. *Massimo* **BISOGNO**, a **guidare questa trasformazione con l'obiettivo di innovare l'amministrazione regionale** e fornire servizi digitali efficienti ai cittadini, alle imprese e ai professionisti nell'ambito di un perimetro di azione sicuro, monitorato e affidabile. «La Regione Campania», ha sottolineato il dott. **BISOGNO**, «ha riconosciuto da tempo l'importanza di cambiare il volto dell'amministrazione pubblica, superando i processi burocratici arcaici e adottando soluzioni digitali per semplificare le interazioni con il territorio».

«Un elemento cruciale è stato l'accento posto sulla sicurezza informatica, resa ancora più evidente dalla pandemia da Covid-19 che ha evidenziato le sfide legate alla protezione dei dati e dei procedimenti amministrativi».

Per affrontarle, sono state intraprese azioni concrete ed effettuati ingenti investimenti. Tra questi figura l'accordo stipulato con l'Università di Salerno - riconosciuta come un'eccellenza nazionale in tema di *Cybersecurity* - volto a rafforzare la capacità degli Uffici Regionali in **misura, prevenzione e gestione del rischio informatico**, anche attraverso l'implementazione di un sito di "*Disaster Recovery*" e la creazione di un'*Academy* dedicata all'alta formazione in ambito *Cybersecurity*.

Altro aspetto fondamentale sul quale si è posta l'attenzione nel corso dell'intervento è la **resilienza umana alla *cybersecurity***: infatti, «il problema della sicurezza è nella maggioranza dei casi legato a comportamenti non corretti da parte degli esseri umani». In virtù di ciò, la Regione ha avviato un programma di formazione triennale per sensibilizzare i dipendenti regionali in merito all'importanza della sicurezza informatica.

Per garantire, invece, un controllo costante e una risposta tempestiva alle minacce informatiche, è stato istituito il *Security Operation Center*, un nucleo regionale interno che monitora attentamente i sistemi informatici dell'amministrazione e che interviene in via preventiva o a seguito di segnalazioni di anomalie. La Regione Campania sta investendo anche nella ristrutturazione del suo *Data Center*, che sarà certificato secondo gli standard ISO 9001 e ISO 27001. Grazie anche alla collaborazione con il Polo Strategico Nazionale (PSN), «l'amministrazione regionale si candida ad ospitare i dati degli enti locali, in particolare quelli delle aziende ospedaliere, garantendo un alto livello di sicurezza informatica».

In conclusione, gli investimenti in ambito di connettività, trasformazione digitale e sicurezza informatica rappresentano una priorità regionale. Grazie anche al Programma Regionale FESR 2021-2027, che assegna alla tematica della digitalizzazione risorse per oltre 200 milioni di euro - e in armonia con quanto previsto dal PNRR, che per gli interventi di *Cybersecurity* ha programmato interventi complessivi per oltre 600 milioni di euro - **l'amministrazione regionale sta aprendo la strada a un futuro digitale più promettente**, sicuro ed efficiente per l'intero territorio campano.

[L'articolo è tratto dall'intervento del dott. *Massimo* **BISOGNO** tenuto nel corso del seminario "Transizione 4.0 @ Cybersecurity"**]**

◂ Dott. *Massimo* **BISOGNO**, Direttore dell'Ufficio Speciale per la crescita e la transizione al digitale presso Regione Campania

RIVEDI IL SUO INTERVENTO

Elaborazione a cura di
Angela **MASTRILLI** e *Marialaura* **SALVIA**

DIGITALIZZAZIONE, TELEMEDICINA, FASCICOLO SANITARIO ELETTRONICO: VERSO UN SERVIZIO SANITARIO PIÙ VELOCE, EFFICIENTE E SICURO

La trasformazione digitale dei servizi sanitari è un tassello fondamentale nella sfida al cambiamento culturale e fonda la sua strategia sui *driver* dell'interoperabilità, dell'integrazione nel processo di cura e della sicurezza di dati, sistemi e reti.

La via verso la digitalizzazione è stata in gran parte tracciata da modelli di successo quali l'*E-Commerce* e l'*E-Banking*. Tuttavia, nel settore sanitario, l'applicazione di norme e regole dirette a tutelare la riservatezza dei dati personali e sensibili appare spesso in contrasto con le esigenze di rapidità, di urgenza, di garanzia di salute del paziente e spesso la protezione della *privacy* viene percepita come un limite invalicabile alla piena digitalizzazione dei processi.

«L'obiettivo per l'*E-Health* è replicare i modelli digitali di successo» - afferma il prof. *Enrico* **COSCIONI**, Presidente dell'Agenzia Nazionale per i Servizi Sanitari Regionali (AGENAS) - «utilizzando quanto di più sofisticato attualmente disponiamo per garantire **protezione e riservatezza *online*** (per es. i conti *on line*) e applicando specifiche procedure di valutazione di impatto (DPIA) e rischio del trattamento».

Il Servizio Sanitario Nazionale (SSN) sta investendo da diversi anni, tra l'altro, sul Fascicolo Sanitario Elettronico (FSE) e sulla Piattaforma di Telemedicina: «piattaforme mutuamente connesse che concorrono nel realizzare processi clinici, di governo tecnologico, di raccolta dati e messa a disposizione di servizi verso utenti e professionisti», afferma il prof. **COSCIONI**.

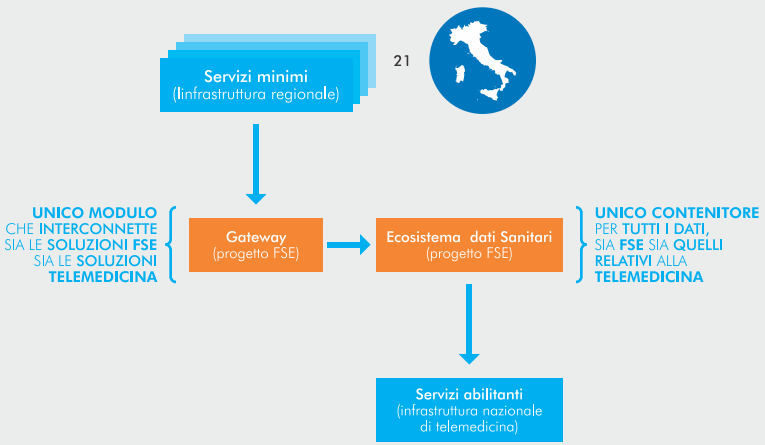
L'uso di soluzioni innovative introdotte con la **telemedicina** consente agli operatori sanitari di assistere pazienti ovunque essi siano, favorire la deospedalizzazione, migliorare le cure e favorire la personalizzazione delle terapie, anche grazie alla condivisione dei dati clinici reperibili dal Fascicolo Sanitario Elettronico del paziente.

Fondamentale nel percorso fin ad ora intrapreso è stato l'operato svolto dall'AGENAS - organo tecnico scientifico del SSN - che ha garantito omogeneità ed efficienza alle politiche di digitalizzazione dei servizi sanitari. Dal 2022 nel ruolo di Agenzia Nazionale per la Sanità Digitale (ASD), l'AGENAS è stata chiamata a gestire l'attuazione degli investimenti della Misura 6 - Salute del PNRR, per quanto attiene lo sviluppo e implementazione della Piattaforma Nazionale di Telemedicina (PNT).

Con funzioni di governo e di validazione dell'Ecosistema di Dati Sanitari (EDS), connessa con i verticali di Telemedicina regionali che realizzano i servizi minimi, la PNT ha la finalità di **semplificare i percorsi diagnostici e terapeutici assistenziali**. Ambiti di intervento, questi ultimi, fortemente congiunti sia con il potenziamento del FSE che con lo stesso PNRR.

Emergono chiaramente i rischi connessi alla centralità che la telemedicina assumerà nei prossimi anni. Ampliandosi nelle possibilità applicative (si pensi, ad esempio, alla progressiva introduzione di dispositivi indossabili intelligenti) e nella quantità e qualità di dati da gestire (l'impiego di algoritmi di *machine learning* per lo *screening* e la diagnosi precoce), i **servizi sanitari digitalizzati si presteranno sempre più a potenziali criticità di *cybersecurity***: dalla riservatezza dei dati sanitari sensibili del paziente conservati nelle piattaforme *cloud*, all'affidabilità dei dispositivi medici elettronici utilizzati nelle prestazioni sanitarie o indossati dal paziente, alla sicurezza delle informazioni che si trasmettono attraverso dispositivi e reti cui sono connessi.

Figura 1 - FSE & Telemedicina: un'architettura integrata (Fonte: sito Agenas)



Potenziale di rischio che risulta inevitabilmente ampliato se il modello per il coordinamento della presa in carico della persona e per il raccordo tra servizi e professionisti coinvolti nei diversi *setting* assistenziali è di tipo distribuito, basato cioè su sistemi di assistenza domiciliare integrata e sulla realizzazione di Centrali Operative Territoriali (COT). Alla flessibilità operativa e a una più efficace capacità di risposta del sistema rispetto agli specifici contesti applicativi, corrisponde un'intrinseca *exposure* per la maggiore varietà e variabilità dei singoli componenti e le necessarie connessioni.

«Tutto ciò», osserva il prof. **COSCIONI**, «impone una standardizzazione di procedure, regole e strumenti e la necessaria omogeneità di competenze, considerato che l'attaccante predilige i punti deboli del sistema in termini di competenze di analisi, risorse utilizzate per il monitoraggio e capacità risposta (es. poliambulatori)».

Invero, **quello della sanità è stato, nel corso del 2022 e a livello mondiale, il secondo settore più colpito dagli attacchi informatici**: il mercato nero dei dati sanitari è fiorente dal momento che - nell'ambito del *dark web* - una cartella sanitaria può arrivare a costare anche 2.000 dollari. Ciò che sicuramente può e deve preoccupare è il dato secondo il quale gli attacchi con impatti gravi sulle strutture sanitarie sono oltre il 70%; valore che raggiunge il 78% dei casi in Italia ove, negli ultimi quattro anni, le aggressioni risultano triplicate a fronte di una ridotta capacità di reazione delle strutture interessate (fonte: Rapporto Clusit 2023).

«In tale quadro l'AGENAS, nel proporsi di favorire una piena e sicura transizione digitale del SSN e nel promuovere la disponibilità degli strumenti digitali a supporto di erogatori, operatori e utenti dei servizi sanitari, intende contribuire a valorizzare modelli e soluzioni, nonché a diffondere consapevolezza e *best practies* in materia di protezione, conservazione e diffusione dei dati relativi alla salute delle persone a favore degli organismi sanitari pubblici e privati, degli esercenti la professione sanitaria e dello stesso paziente».

[**L'articolo è tratto** dall'intervento del prof. *Enrico* **COSCIONI** tenuto nel corso del seminario "Transizione 4.0 @ Cybersecurity"]

◂ Prof. *Enrico* **COSCIONI**,
Presidente AGENAS
Agenzia Nazionale
per i Servizi Sanitari Regionali

RIVEDI IL SUO INTERVENTO

#CRITICAL NETWORK INFRASTRUCTURE #CYBERWARFARE
#ATTACCHI HACKER #SICUREZZA INFORMATICA

Elaborazione a cura di
Nadia **ESPOSITO** e *Sabatino* **CATUOGNO**

L'ERA DELLA CYBERWARFARE: LE MISURE A TUTELA ED IMPLEMENTAZIONE DEGLI ASSET STRATEGICI DI DIFESA

Il seminario "Transizione 4.0 @ Cybersecurity: lo spazio di azione tra metodi di Vulnerability Assessment e strumenti per la Data Protection" ha rappresentato una preziosissima opportunità per condividere alcune riflessioni sulla Cybersicurezza Nazionale, tema strategico in uno scenario globale caratterizzato da Infrastrutture Informative Critiche (*Critical Network Infrastructure* - CNI) sempre più digitalizzate e interoperabili. I fondamentali settori delle società moderne, Economia, Energia, Trasporti, Telecomunicazioni, Salute, sono infatti settori gestiti da reti dipendenti e interconnesse, necessarie a garantire il corretto svolgimento della vita degli Stati e delle comunità.

Ciò impone una maggiore e diversa attenzione - oltre che per ogni singola CNI e per l'insieme delle CNI nazionali - anche a tutti gli aspetti di protezione e sicurezza. Dopo terra, mare, cielo e spazio, **il nuovo dominio della conflittualità è lo spazio cibernetico**. Seppur in continua evoluzione, ad oggi è considerato il migliore scenario per la guerra fra Stati (*cyberwarfare*).

Del tutto inimmaginabile fino ad un ventennio fa, se non per gli autori di fantascienza, un attacco informatico su scala internazionale oggi può essere in grado di generare un danno alle infrastrutture strategiche di un paese, ai suoi stessi sistemi di difesa, oltre che a qualunque altro strumento informatico utilizzato per la sicurezza.

L'evoluzione delle tecnologie digitali, la diffusione delle reti, l'aumento degli scambi elettronici, nonché la possibilità di virtualizzare i sistemi di comando e controllo del modo reale, hanno reso sempre più facili le intrusioni degli *hacker* e gli attacchi informatici. La sicurezza informatica, dunque, è diventata un tema centrale per la difesa degli interessi nazionali e per la sicurezza delle persone.

«Crescono in modo esponenziale i tentativi di attacchi informatici su reti classificate e non classificate della Difesa, di altri Ministeri, di Enti Governativi e non Governativi. In particolare, sono i Paesi a regime non democratico i principali protagonisti di questa minaccia. Ad affermarlo è il Sen. *Nicola* **LATORRE**, Politico e Politologo italiano, Docente in Politica Estera e Difesa Italiana presso la Luiss Guido Carli e, dal 2020, Direttore Generale dell'Agenzia Industrie Difesa.

«Questi Paesi», continua il Senatore, «stanno affinando la loro attività di spionaggio e la loro capacità di intervenire in termini di disinformazione, utilizzando in maniera efficace i propri agenti *hacker* e gli attacchi informatici». Tale pressione informatica si concentra sulle infrastrutture strategiche, generando conseguenze anche dal punto di vista economico-sociale.

Ai sabotaggi, attacchi e incidenti informatici, si aggiunge l'utilizzo delle capacità informatiche per **minare la sicurezza nazionale** utilizzando, ad esempio, lo strumento della disinformazione. «Si è visto come, di recente, anche le lezioni in grandi Paesi siano state condizionate da attività di questo tipo, insidiando le tenute democratiche dei Paesi».

«La situazione in Italia non è all'anno zero, poiché il sistema di difesa del nostro Paese ha operato in maniera tempestiva ed efficace», attuando tutte le contromisure necessarie per una efficace gestione del rischio tra cui:
- l'avvio di un monitoraggio costante dei possibili attacchi;
- la costituzione di un comando interforze per le operazioni cibernetiche;
- la partecipazione attiva alle più importanti operazioni di sicurezza e stabilizzazione in campo internazionale.

◂ Sen. *Nicola* **LATORRE**, Direttore Generale dell'Agenzia Industrie Difesa

RIVEDI IL SUO INTERVENTO

«Non bisogna però mai fermarsi e ritenere che si possa essere soddisfatti di quanto fatto finora», ha affermato **LATORRE**. «È necessario irrobustire le capacità dei *frontline* in grado di lanciare gli *alert* in tempi necessari e sufficienti, nonchè consolidare le capacità di un continuo *audit* dei sistemi.
Così come è fondamentale una strategia condivisa con i nostri alleati, poiché [...] in assenza di una strategia internazionale condivisa, la partita risulta destinata ad essere persa. Da questo punto di vista, il ruolo della NATO è assolutamente fondamentale e strategico».

Per quanto riguarda lo spettro delle tipologie di minacce informatiche, si avverte una sempre maggiore sofisticazione delle azioni poste in essere dai cyberterroristi, tanto da far pensare che i recenti attacchi *cyber* nel conflitto russo-ucraino rappresentino solo un banco di prova, il palcoscenico ove effettuare le prove tecniche di futuri attacchi, relativamente al grado di efficacia e di devastazione.

«È quindi necessario rendere condivisa, nel nostro Paese, una cultura della difesa e della sicurezza che purtroppo rappresenta una oggi delle criticità maggiori», ha sottolineato il Senatore. Il tema della sicurezza informatica richiede un significativo e intenso lavoro volto a incentivare e a finanziare il supporto tecnologico, standardizzare il sistema di regole e accelerare i percorsi di formazione. Tutti questi elementi sono decisivi in una strategia di difesa che non può trascurarne l'indispensabile complementarità.

In definitiva, **la sicurezza informatica assume un ruolo decisivo nello scenario geopolitico attuale**, segnato da una competizione tesa a definire anche le nuove gerarchie e i nuovi equilibri mondiali: «Il settore della sicurezza informatica deve quindi essere considerato una questione strategica necessaria anche a garantire lo sviluppo del Paese», ha concluso **LATORRE**.

[**L'articolo è tratto** dall'intervento del Sen. *Nicola* **LATORRE** tenuto nel corso del seminario "Transizione 4.0 @ Cybersecurity"]

Ringraziamo per le testimonianze:

Ing. *Francesco* **MISTRETTA**,
Amministratore della Technology Advising. Technology Advising S.r.l è specializzata nella progettazione e realizzazione di sistemi di gestione del territorio mirati alla sicurezza dai rischi ambientali e antropici; nell'ambito del system integrator; nella realizzazione e gestione di software e hardware di ausilio alle istituzioni.

Ing. *Fabio* **CORNEVILLI**,
Responsabile tecnico della System Management. System Management è un'azienda parte di Digital Platforms, gruppo industriale italiano che opera nei settori dell'IoT e della Cyber Security, il cui obiettivo è quello di supportare l'evoluzione digitale dei processi aziendali, soprattutto in ambito di Business Consulting, ICT Integration, Software Solutions, Digital Experience Design e Big Data Analysis.


CYBER
WARFARE
EUROPE
ASIA
CHINA
INDIA
KAZAKHSTAN
UZBEKISTAN
TURKMENISTAN
TAJIKISTAN
KYRGYZSTAN
AFGHANISTAN
PAKISTAN
IRAN
NEPAL
OMAN
UKRAINE
FINLAND
SWEDEN
NORWAY
ALGERIA
MOROCCO
ETHIOPIA
UGANDA
KENYA
TANZANIA
ANGOLA
ZAMBIA
MALAWI
MADAGASCAR
MAURITIUS
Reunion (France)
SWAZILAND
SOUTH AFRICA
LESOTHO
SRI LANKA
Arabian Sea
Bay of Ben
Saint Helena (UK)
SOUTH

#SICUREZZA DIGITALE #BUSINESS CONTINUITY
#CYBERSECURITY #INNOVAZIONE TECNOLOGICA
#SVILUPPO TECNOLOGICO

Elaborazione a cura di
Giovanna **CIRILLO** e *Sabrina* **D'ANGELIS**

L'**AZIONE** DELL'**ACN** NEL **PROCESSO** DI **TRANSIZIONE DIGITALE** PER UN **PAESE RESILIENTE**

«La *cybersecurity* è la seconda emergenza in Europa, dopo il cambiamento climatico e prima dell'immigrazione». Riportando questa affermazione del Presidente della Commissione Europea *Jean-Claude Juncker* nel discorso sullo Stato dell'Unione del 13 settembre 2017, *Bruno* **FRATTASI**, Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, ha aperto il suo intervento nel corso del **Seminario "Transizione 4.0 @ Cybersecurity: lo spazio di azione tra metodi di Vulnerability Assessment e strumenti per la Data Protection"**.

Il Direttore di ACN ha così voluto sottolineare che **l'urgenza della sicurezza digitale** - dai perimetri sempre meno regolari e dalle superfici sempre più estese - **è la principale sfida che il mondo occidentale è chiamato ad affrontare nel breve-medio termine**, al netto dell'emergenza pandemica del 2020. Una sfida che include tutti i confini della sicurezza. Per darne una misura, il direttore **FRATTASI** propone l'esempio di un attacco cibernetico ad una grande banca: se non correttamente gestito, potrebbe generare conseguenze sistemiche. In questa ipotesi, la compromessa sicurezza dei sistemi di transazione minerebbe la *business continuity* degli operatori economici e genererebbe un immediato e diffuso rischio di insicurezza anche tra i cittadini, fino ad arrivare al disordine sociale.
Il nostro futuro - e quello dei rapporti umani - dipendono dai rischi che l'ecosistema cibernetico presenta ogni giorno, e quindi dalla capacità di risposta sistemica che si è in grado di dare.

In tale ottica, è stata recentemente ridefinita in Italia l'**architettura nazionale di cybersicurezza**, con l'obiettivo di razionalizzare e semplificare il sistema di competenze esistenti a livello nazionale, valorizzando ulteriormente gli aspetti di sicurezza e resilienza cibernetica, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico. In questo quadro, l'Agenzia si pone al centro dell'ecosistema, a tutela degli interessi nazionali nel campo della cybersicurezza, combinando ricerca e innovazione all'interno di un processo evolutivo in ottica europea.

La *mission* affidata all'Agenzia è soprattutto quella di rafforzare la "*cyber resilienza*" dell'ecosistema cibernetico nazionale, cioè la capacità - a livello di sistema - di prevenire gli incidenti di sicurezza informatica, resistere ad essi ed eseguire il ripristino quando si verificano.

Adeguandosi ai criteri esposti dalla NIS2 (***Network and Information Security 2***), le organizzazioni riescono a dotarsi di *standard* pensati per **mitigare i rischi per la sicurezza digitale**, rischi legati al contagio e alle ricadute sull'intero sistema. Il processo di evoluzione digitale «[...] deve però crescere con delle regole di responsabilità diffusa e sistemica», ha sottolineato *Bruno* **FRATTASI**.

Le responsabilità sono orientate a sviluppare ad affermare la capacità dell'organizzazione di recuperare i dati, evitare l'interruzione del servizio e mitigare i danni complessivi, garantendo, al contempo, una ripresa efficace da eventi informatici avversi.

In tale ottica, la resilienza, allora, «acquisisce una valenza tecnica» descrivibile a partire dai tre pilastri fondamentali della Strategia Nazionale di Cybersicurezza del nostro Paese:

- **Protezione:** intesa come la capacità di assicurare una transizione digitale *cyber* resiliente della Pubblica Amministrazione (PA) e del tessuto produttivo;
- **Risposta:** relativa alla capacità di rispondere alle minacce, agli incidenti e alle crisi *cyber* nazionali, attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale;
- **Sviluppo:** che coincide con l'innovazione e mira a promuovere in maniera sicura le tecnologie digitali, rispondere alle esigenze del mercato, attraverso strumenti e iniziative volte a supportare i centri di eccellenza, le attività di ricerca e le imprese.

Tali obiettivi strategici, suddivisi in 82 misure da implementare entro il 2026, intendono porsi a fondamento del processo di digitalizzazione del Paese e in un'ottica di investimento (e non di costo), alimentatore del progresso culturale sul tema, in un approccio "*whole-of-society*" che coinvolga operatori privati, mondo accademico, società civile e cittadinanza tutta.

◂ Dott. *Bruno* **FRATTASI**, Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale

RIVEDI IL SUO INTERVENTO

In tale prospettiva, l'Agenzia sta attivando una rete di collaborazioni stabili finalizzate a promuovere, supportare e incentivare **l'innovazione e lo sviluppo tecnologico** (TTOs, Incubatori, Acceleratori), finanziando lo sviluppo di nuove imprese e il trasferimento di risultati della ricerca verso l'impresa nel settore della cybersicurezza. A questo si aggiungono le opportunità derivanti dal Piano Nazionale di Ripresa e Resilienza, tramite il quale mettiamo a disposizione 623 milioni di euro per potenziale lo sviluppo *cyber* del Paese.

L'Agenzia intende quindi porsi al centro di un sistema che deve stimolare la ricerca e l'innovazione per acquistare una maggiore capacità di essere, come Paese, al centro di un processo mondiale: con la crescita della nostra industria tecnologica, infatti, «cresce la sua capacità di essere ascoltata, di essere un *competitor* effettivo nel mercato digitale europeo», conclude il Direttore Generale di ACN.

[**L'articolo è tratto** dall'intervento del dott. *Bruno* **FRATTASI** tenuto nel corso del seminario "Transizione 4.0 @ Cybersecurity"]

#CYBER-CRIME #CYBER-ESPIONAGE
#STRATEGIA NAZIONALE DI CYBERSICUREZZA
#MINACCE CYBER

A cura di
Luca **MARANIELLO** e *Flavia* **PUGLIA**

ANALISI DEI **DRIVER** DI **PERFORMANCE** PER LA **CYBERSECURITY** E **POSSIBILI TRAIETTORIE** DI **IMPROVEMENT** CON IL **PROGETTO STRATEGICO REGIONALE** "MANIFATTUR@ CAMPANIA: INDUSTRIA 4.0"

All'interno di un panorama in costante mutamento - che vede l'evoluzione tecnologica segnata dai processi di transizione digitale accompagnata dall'insorgere per imprese e cittadini, di nuovi potenziali rischi, dalle enormi conseguenze sul piano economico, sociale e politico - è fondamentale attivarsi a livello di Paese al fine di delineare e implementare *policy* di prevenzione e di contrasto, nonché di mitigazione e monitoraggio delle minacce alla sicurezza dello spazio cibernetico.

Siano esse volte ad ottenere profitti illeciti (*cyber-crime*), generare vantaggio informativo per fini di competizione geopolitica (*cyber-espionage*), diffondere narrative non veritiere, ovvero divisive e polarizzanti (*fake news*) in aderenza a specifiche motivazioni politico-economiche, nessuna organizzazione, pur tecnologicamente equipaggiata e proceduralmente preparata, può ambire a eliminare del tutto le minacce che promanano dallo spazio cibernetico.

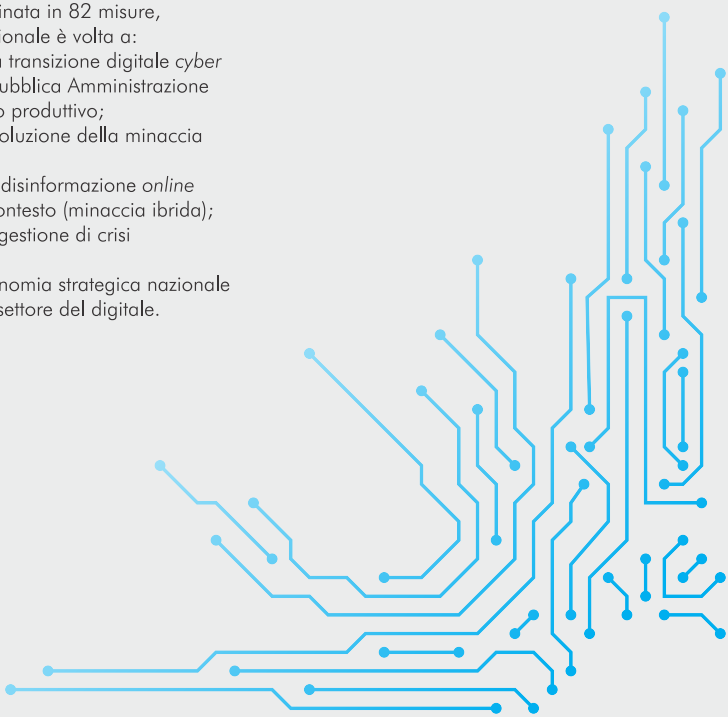
La diffusa consapevolezza della *cybersecurity* come fattore abilitante per lo sviluppo digitale ha reso sempre più pressante la necessità di pianificare, coordinare e attuare misure tese a rendere i sistemi più sicuri e resilienti per il dominio digitale, assicurando, al contempo, la fiducia degli utenti (attori istituzionali, imprese private, pubbliche amministrazioni e cittadini) nella possibilità di sfruttarne i relativi vantaggi, nella piena tutela dei diritti e delle libertà fondamentali.

L'obiettivo da perseguire è, pertanto, duplice: da un lato, definire ruolo, responsabilità e risorse per gli attori che a vario titolo concorrono a popolare l'ecosistema della cybersicurezza (istituzioni, operatori delle infrastrutture critiche, del mondo dell'università e della ricerca, del sistema delle imprese e della società civile). Tali attori sono chiamati, quindi, a delineare e implementare le singole azioni che concorrono a potenziare la sicurezza digitale.
Dall'altro, disporre di un set di indicatori che consentano di mappare l'*assessment* della sicurezza tecnologica, monitorarne eventuali livelli di sviluppo/criticità secondo una precisa metodologia di rilevazione e, in una prospettiva di *accountability*, di valutare e attualizzare strategia e azioni.

L'azione sinergica di tale ecosistema ha portato, in Italia, all'elaborazione della **Strategia Nazionale di Cybersicurezza 2022-2026**, la cui attuazione è affidata alla Agenzia per la Cybersicurezza Nazionale. Declinata in 82 misure, la Strategia Nazionale è volta a:
- assicurare una transizione digitale *cyber* resiliente della Pubblica Amministrazione (PA) e del tessuto produttivo;
- anticipare l'evoluzione della minaccia *cyber*;
- contrastare la disinformazione *online* nel più ampio contesto (minaccia ibrida);
- supportare la gestione di crisi cibernetiche;
- favorire l'autonomia strategica nazionale ed europea nel settore del digitale.

Suddette sfide sono affrontate con la definizione di modelli, azioni e indicatori di monitoraggio delle attività e del *cyber assessment* di Istituzioni, operatori privati e società civili, organizzati al fine di assicurare una concreta implementazione della strategia sia dal punto di vista organizzativo che attuativo.

In particolare, la misura n° 82 della Strategia, prevede la definizione di **Metriche e Key Performance Indicators** (KPI), atti a misurare i progressi effettivamente compiuti per potenziare la resilienza cibernetica del paese rispetto a:
- l'efficacia delle Misure di protezione (MP), delle Misure di risposta (MR) e delle Misure di Sviluppo (MS);
- lo sviluppo di Fattori abilitanti (FA) ovvero Formazione, Promozione della cultura della sicurezza cibernetica, Cooperazione.



Il raggiungimento e la messa in atto di tali *good practice*, così come la strutturazione di processi atti a monitorare i KPI sopra elencati, non sono sempre obiettivi immediatamente raggiungibili.
Non sono infatti poche le realtà dell'ecosistema della *cybersecurity* che, per tradizione e/o dimensione, presentano un elevato *gap* di competenze digitali e/o non riescono a sviluppare percorsi di innovazione per valorizzare e proteggere (ulteriormente) il proprio capitale digitale. Attori che rappresentano oggi, per la cronica debolezza, sempre più i bersagli attraverso cui minare i sistemi digitali di realtà più complesse e critiche.

A tal fine, con il Progetto Strategico Regionale "**Manifattur@ Campania: Industria 4.0**", la Regione Campania intende, tra l'altro, supportare gli attori dell'ecosistema regionale della *cybersecurity* nella progettazione e nell'attuazione di processi volti a monitorare e consolidare la sicurezza informatica dei sistemi aziendali e la diffusione di una cultura della resilienza digitale, conformemente ai parametri europei e alla Strategia Nazionale.

Ciò è perseguito attraverso un sistema integrato di interventi, tra cui lo sviluppo della **Rete Regionale dei laboratori 4.0** (**R²Lab**$_{4.0}$) che - coordinata da Fondazione Idis-Città della Scienza - intende sistematizzare l'offerta regionale dei servizi ad intensità di conoscenza nel supporto della transizione 4.0.

In particolare, il nodo della rete specializzato in *cybersecurity* - gestito dal Dipartimento di Informatica dell'Università degli studi di Salerno - presenta, nell'attuale offerta, l'erogazione di servizi atti a supportare le PMI e la PA in attività legate all'Archiviazione e notarizzazione mediante tecnologie di *blockchain*, così come la definizione di *Identity* e *authentication tools* per il *secure web*, ma anche servizi più semplici e di immediata applicazione come quelli di *Security Risk Analysis* a supporto del *Vulnerability Assessment* e del *Penetration Testing*, servizi per la *Security & Privacy Compliance* e servizi per il Potenziamento della *Secure Network*.

Nel rispetto dell'intrinseca trasversalità e al fine di concorrere a potenziare la resilienza dell'ecosistema campano nei confronti delle minacce, incidenti e crisi *cyber*, le suddette dimensioni di azione saranno opportunamente correlate con interventi atti a delineare, in coordinamento con operatori pubblici e privati del territorio, piani di gestione della crisi (prassi, strumenti e azioni), processi che strutturano le best *practice* in ambito *cyber* e protocolli di monitoraggio delle infrastrutture locali da divulgare e utilizzare.

Il risultato atteso è assicurare lo sviluppo, in modo consapevole e sicuro, delle tecnologie digitali in grado di rispondere alle esigenze del mercato e dei cittadini. Il contributo è, da un lato, quello di consentire al territorio campano di essere sempre più competitivo e all'avanguardia sui pilastri degli attuali paradigmi tecnologici; dall'altro, quello di concorrere a rafforzare il perimetro della sicurezza nazionale.

INDICATORE DELLA **STRATEGIA NAZIONALE** DI **CYBERSICUREZZA** 2022-2026	**DIMENSIONE** DI **INTERESSE**	**INTERVENTO PREVISTO** DAL **P. S. R. MANIFATTUR@ CAMPANIA: INDUSTRIA 4.0**
N. operatori che hanno adottato procedure, processi e strumenti definiti con l'obiettivo di assicurare la continuità operativa delle reti, dei sistemi informativi e dei servizi informatici	RISPOSTA	**1.1.2** · Audit dei fabbisogni tecnologici per la transazione 4.0 delle PMI
N. addetti coinvolti nei processi di monitoraggio e situational awareness ivi inclusa l'analisi di minacce, vulnerabilità e attacchi	PROTEZIONE	
N. iniziative promosse per rafforzare le capacità di deterrenza in ambito cibernetico, in ragione degli scenari	SVILUPPO	**2.1.2** · I4.0 Assessment
N. di iniziative di ricerca e sviluppo relative alla cybersicurezza, con particolare riferimento alle startup e alle PMI innovative	SVILUPPO	**2.2.2** · Anima PoC4.0
N. di prodotti e processi informatici di rilevanza strategica sviluppati a seguito di specifiche iniziative progettuali	SVILUPPO	**4.1.2** · Co-design 4.0
N. di progetti realizzati o promossi per supportare lo sviluppo di capacità, tecnologie e infrastrutture di cybersicurezza, mediante l'accesso ai programmi di finanziamento regionali, nazionali, UE	SVILUPPO	**2.1.4** · Potenziamento dei nodi R2Lab4.0
Ammontare dei Finanziamenti erogati per la componente di cybersicurezza	SVILUPPO	**2.1.5** · Progetti Pilota per la prequalifica ed assesment dei servizi della R2Lab4.0
N. iniziative volte a rafforzare la cybersicurezza nella PA	SVILUPPO	**4.1.2** · Co-design 4.0
N. imprese e startup sostenute nelle attività di progettazione e realizzazione di prodotti e servizi ad alta affidabilità	SVILUPPO	**2.2.3** · ACCI4.0
N. imprese campane che offrono prodotti e servizi di cybersecurity	SVILUPPO	**1.1.2** · Audit dei fabbisogni tecnologici per la transazione 4.0 delle PMI
N. di start-up operanti nel settore della cybersecurity	SVILUPPO	
N. iniziative per lo sviluppo di start-up operanti nel settore della cybersecurity	FATTORE ABILITANTE	**4.1.1** · Attrazione, sviluppo e retention di start up e talenti
N. iniziative volte ad incentivare partnership pubblico-privato con aziende di cybersecurity	FATTORE ABILITANTE	**4.1.2** · Co-design 4.0
N. percorsi formativi di specializzazione in cybersecurity sviluppati per il personale docente	FATTORE ABILITANTE	**3.1.1** · Scuola 4.0
N. di corsi post-diploma (ITS) di specializzazione in cybersecurity sviluppati	FATTORE ABILITANTE	**3.2.1** · Skilling on the Lab4.0
N. di dottorati di ricerca e master in cybersecurity sviluppati	FATTORE ABILITANTE	**2.1.5** · Progetti Pilota per la prequalifica ed assesment dei servizi della R2Lab4.0
N. Istituti che hanno sviluppato iniziative per la promozione dell'educazione digitale, comprensiva di aspetti di sicurezza cibernetica	FATTORE ABILITANTE	**3.1.1** · Scuola 4.0
N. iniziative volte a promuovere l'educazione digitale anche in raccordo con il mondo accademico, comprensive di aspetti di sicurezza cibernetica	FATTORE ABILITANTE	**3.2.1** · Skilling on the Lab4.0
N. soggetti coinvolti in iniziative per la promozione dell'educazione digitale, comprensiva di aspetti di sicurezza cibernetica	FATTORE ABILITANTE	**3.1.1** · Scuola 4.0
N. iniziative volte alla definizione di policy (private) di divulgazione coordinata di vulnerabilità	FATTORE ABILITANTE	**5.1.2** · Iniziative di promozione e diffusione dei risultati dei processi di trasformazione 4.0
N. iniziative di sensibilizzazione sviluppate per favorire l'applicazione del Framework Nazionale per la Cybersecurity e la Data Protection e dei Controlli essenziali di cybersecurity ad uso delle PA e delle imprese	PROTEZIONE	
N. iniziative che mirano a comunicare l'effettivo livello della minaccia cyber.	PROTEZIONE	**1.1.4** · Azioni informative I4.0
N. iniziative volte a porre in essere un'azione di coordinamento nazionale per prevenire e contrastare la disinformazione online	PROTEZIONE	

▲ Nella tabella precedente, le possibili correlazioni tra alcuni KPI forniti dalla Strategia Nazionale di Cybersicurezza e gli interventi previsti dal progetto "**Manifattur@ Campania: Industria 4.0**".

SCOPRI LA
RETE REGIONALE
DEI LABORATORI 4.0 ($R^2LAB_{4.0}$)

#ATTACCHI HACKER #CYBERSECURITY #CYBER RISK
#DIGITAL TRANSFORMATION #TECNOLOGIE 14.0

A cura di
Luca **SIMEONE** e *Valeria* **LIGUORI**

CYBERSICUREZZA: QUALE RUOLO DELLA FORMAZIONE?

I recenti attacchi *hacker* su scala internazionale che hanno colpito anche l'Italia, sancendo la necessità di disporre di competenze adeguate all'implementazione di strategie di prevenzione delle minacce alle infrastrutture digitali, rappresentano un'occasione per riflettere sull'offerta in tema di cybersicurezza del sistema della formazione per studenti e lavoratori.

Il tema della *Cybersecurity* rappresenta una delle grandi sfide della quarta rivoluzione industriale: esso impatta non solo sulla tenuta dei grandi *asset*, reti pubbliche, archivi sensibili, dati per la sicurezza nazionale, ma anche sulle PMI e su tutti noi, nel quotidiano.

Lo scorso 5 febbraio un massiccio attacco *hacker*, attraverso un ***ransomware***, ha colpito molti sistemi informatici in tutto il mondo, Italia inclusa, bloccando reti e sistemi, nonché l'accesso ai relativi contenuti. L'Agenzia per la Cybersicurezza Nazionale (ACN), l'autorità che si occupa di implementare la Strategia Nazionale di Cybersicurezza, ha rilevato come siano state decine le realtà che hanno riscontrato un'attività malevola nei loro confronti. I recenti fatti hanno, in qualche modo, riacceso i riflettori su un tema: la formazione sul contrasto agli attacchi informatici.

Attualmente, la nostra nazione vive una situazione emergenziale strutturale legata allo *skill shortage* in ambito ITC sia per le competenze di base - il 54% della popolazione italiana non possiede competenze digitali di base (fonte: Rapporto DESI 2022) - sia per quelle avanzate - l'Italia è ultima in UE per numero di iscritti a corsi di laurea in materia ICT in rapporto alla popolazione: 0,7 ogni mille abitanti, contro i 5,3 della Finlandia, *leader* in Europa (cfr. Ambrosetti, *Next Generation DigItaly*, 2022); inoltre, solo il 40% dei lavoratori ha ricevuto una formazione specifica sulla sicurezza cibernetica (fonte: Rapporto Censis - *DeepCyber*, Aprile 2022).

Un tipo di educazione, quest'ultima, su cui gli Istituti Tecnologici Superiori (ITS) e le Università possono giocare un ruolo importante. I percorsi professionalizzanti, i *Master* e le *Academy* sempre più risultano orientati nello sviluppare competenze e trasferire *know-how* specialistici in grado di supportare imprese e pubbliche amministrazioni.

Un aiuto concreto, insomma, per:
- l'analisi di vulnerabilità dei sistemi informatici e per le possibili conseguenze derivabili da un'intrusione;
- la predisposizione di adeguati piani di sicurezza e riservatezza a supporto della continuità operativa;
- lo sviluppo di strategie di comunicazione per la gestione del danno di immagine e reputazionale.

Rispetto a tali tematiche, gli ITS offrono già percorsi *ad hoc*. In particolare, gli Istituti che si occupano di Tecnologie dell'Informazione e della Comunicazione (ITC) - 11 in totale in Italia - presentano, nella propria offerta formativa, corsi di "*Cybersecurity*", "*Cyber Degence*" e "Sicurezza informatica".
Anche gli Istituti Tecnologici Superiori attinenti ad altri ambiti formativi - come, ad esempio, le Nuove Tecnologie per il *Made in Italy* - prevedono percorsi tesi a formare *Cybersecurity specialists* con moduli in materia gestione del *cyber risk*, tecniche di difesa e logiche di funzionamento di architetture IT complesse. Inoltre, è attiva in Italia la Rete di Coordinamento Nazionale degli Istituti Tecnologici Superiori per la Transizione Digitale che vede anche la partecipazione di soggetti istituzionali, quali Regioni, Associazioni di categoria e l'Agenzia per la Cybersicurezza Nazionale.
Tutti gli attori tendono alla promozione e allo sviluppo di percorsi formativi dedicati alla digitalizzazione e alla sicurezza informatica dei processi, sia delle imprese private che della Pubblica Amministrazione.

Una tale ampiezza dell'offerta formativa e la dichiarata intenzione delle imprese a dotarsi di competenze in materia di sicurezza informatica (il *Cybersecurity Engineer* è tra le 25 professioni più richieste in Italia secondo i dati del Report Linkedin Lavori in Crescita 2023), trova sintesi nell'elevato tasso di *placement* dei diplomati nei percorsi ITS in materia di ICT che ha raggiunto l'82% (fonte: Indire, Banca dati nazionale ITS - aprile 2022), anche grazie al coinvolgimento di formatori provenienti dal mondo del lavoro (8 su 10 in termini di ore) e alla formazione *on the job* (40% delle ore totali dedicate agli stage).

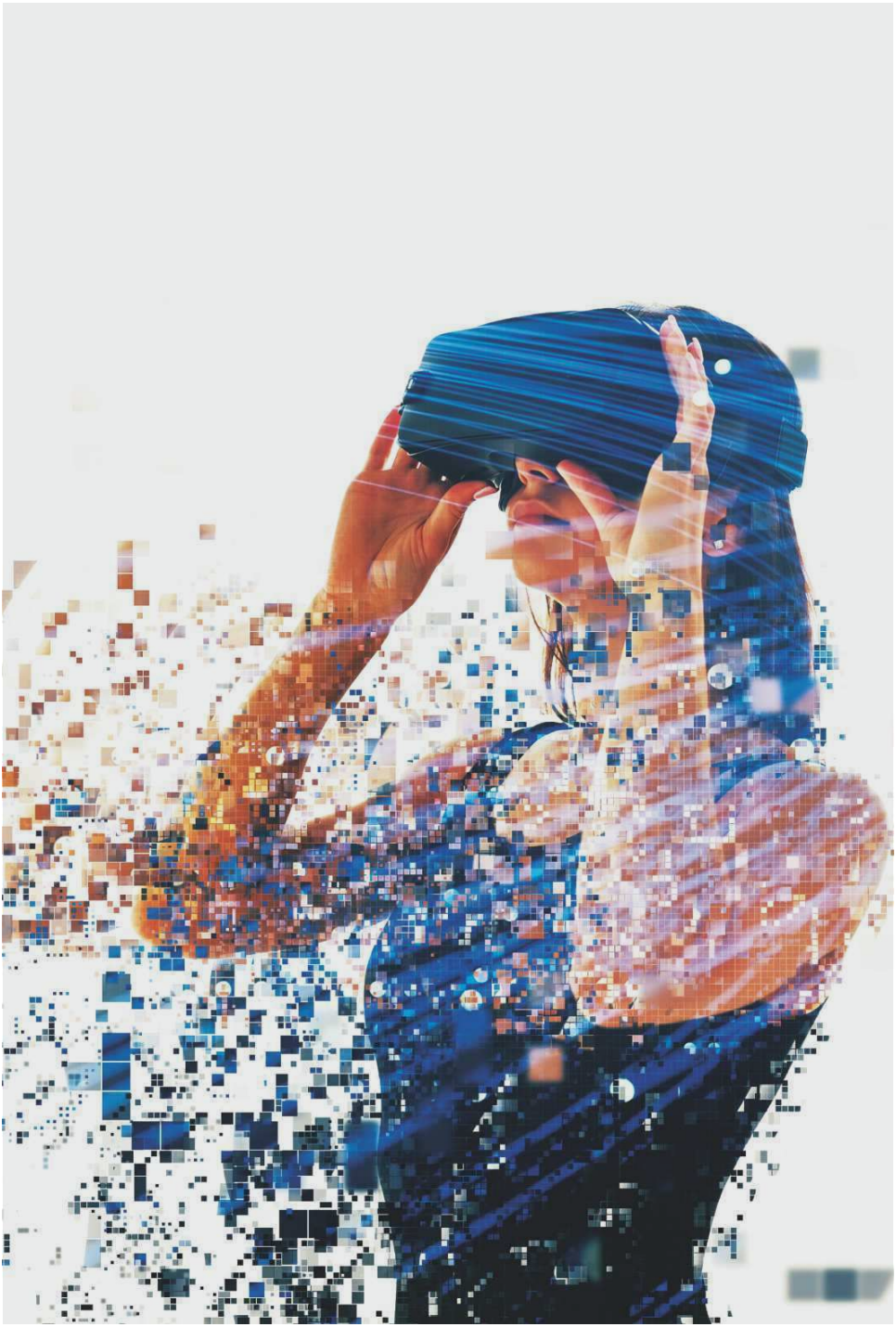
Pur scontando un ritardo nell'attivazione di percorsi di formazione terziaria nell'area ITC (fonte: Rapporto INDIRE, aprile 2022), partiti solo nel 2023, la Campania si caratterizza, al pari delle principali regioni italiane, per un'ampia e diversificata offerta formativa universitaria e post-laurea in materia di *cybersecurity*.
Recente è l'apertura da parte di *Intellera Consulting* - in collaborazione con *PricewaterhouseCoopers* - di un *open space* presso l'Università degli Studi di Salerno, in cui i professionisti delle due società di consulenza opereranno nei prossimi tre anni a fianco di 180 giovani neolaureati e laureandi dell'ateneo. L'obiettivo è quello di lavorare su programmi nazionali e internazionali in ambito di *Digital Transformation* e *Data Science*, con un focus specifico sulla *Cybersecurity*. Tale iniziativa arricchisce l'offerta formativa specialistica post-laurea in Campania che conta: il master in "*Leadership and Digital Transformation*" presso l'Università degli Studi di Salerno, in collaborazione con il Centro Alti Studi per la Difesa; il Dottorato in *Information Engineering* - Curriculum in *Cybersecurity* - presso l'Università degli Studi di Napoli Parthenope; e la *Cyber HackAdemy* con cui l'Università di Napoli Federico II, in collaborazione con Accenture, si propone di formare esperti su tematiche di sicurezza informatica in presenza di architetture di rete avanzate, seguendo un approccio formativo di tipo *hands-on* e metodi di apprendimento basati su sfide (*Challenge Based Learning* - CBL) rispetto a differenti contesti applicativi (*Automotive, Manufacturing, Media, Energy, E-Health, Public Safety, Smart Cities*).

PARTECIPA ALLA MANIFESTAZIONE DI INTERESSE · AZIONE 3 · ORIENTAMENTO E FORMAZIONE IN AMBITO INDUSTRIA 4.0

L'interesse del sistema della formazione e la tradotta capacità di sviluppare competenze coerenti con l'evoluzione dei fenomeni di cybersicurezza, per gli studenti di ogni ordine e grado, non trova equivalenti nei percorsi di formazione continua dei dipendenti di imprese e pubbliche amministrazioni. Ancora ridotte rispetto al bacino di utenti e agli impatti prospettati, risultano - a livello nazionale - le esperienze tese a migliorare, sviluppare e riqualificare le *skill* dei lavoratori, attraverso un *upgrade* delle abilità possedute in ambito digitale (*up-skilling*), ovvero di apprendimento di nuove competenze lavorative al fine di ricoprire un nuovo ruolo o un diverso compito (*re-skilling*). Di qui la necessità di promuovere la partecipazione diffusa di Enti di formazione, Agenzie per il Lavoro e PMI per la progettazione di percorsi professionalizzanti specialistici di carattere strategico e tecnico-operativo a favore dei lavoratori per lo sviluppo di competenze 4.0.

Partendo da tale *gap*, trova oggi piena attuazione l'intervento "**3.1.2 - Upskill 4.0**" del Progetto Strategico Regionale "**Manifattur@ Campania: Industria 4.0**", finalizzato alla progettazione partecipata di percorsi di formazione professionalizzanti specialistici a favore delle PMI. I percorsi, sia quelli strategici che quelli di carattere tecnico-operativo, intendono offrire rispettivamente una panoramica sulle nuove tecnologie che rendono un prodotto digitale, un processo automatizzato e controllato, un'infrastruttura digitale sicura: ovvero, consentono al formando di sviluppare una esperienza pratica con l'applicazione *on field* delle nuove tecnologie I4.0, tra cui quelle dedicate alla *cybersecurity*.

Nell'ottica di favorire la più ampia partecipazione, si chiede agli *stakeholders* qualificati del sistema educativo di istruzione e di formazione, del sistema delle professioni e del sistema delle imprese a partecipare ad occasioni di confronto sui temi relativi alle trasformazioni del lavoro, delle professioni e delle competenze a supporto e indotte della/dalla transizione 4.0 del sistema dell'innovazione regionale.



PARTECIPA AL **PROGETTO**

Il **Progetto Strategico Regionale** "Manifattur@ Campania: Industria 4.0" intende offrire un nuovo impulso alla transizione 4.0 dell'economia regionale attraverso azioni integrate che, attuate da **Fondazione Idis-Città della Scienza**, permetteranno di qualificare l'offerta regionale di servizi ad alta intensità di conoscenza, di rafforzare la capacità delle PMI campane, di sviluppare e/o adottare nuovi processi/prodotti, di divulgare e diffondere presso il mercato e la collettività l'impiego sostenibile delle tecnologie abilitanti il paradigma dell'**Industria 4.0**.

SEGUICI SUI **CANALI SOCIAL**

AZIONE 1
COORDINAMENTO
DEGLI **STAKEHOLDERS RILEVANTI**
DELL'**ECOSISTEMA CAMPANIA 4.0**

PARTECIPA

AZIONE 2
SUPPORTO AI **PROCESSI**
DI **TRANSIZIONE 4.0**
DELL'**ECOSISTEMA REGIONALE**

PARTECIPA

AZIONE 3
ORIENTAMENTO
E **FORMAZIONE**
IN **AMBITO INDUSTRIA 4.0**

PARTECIPA

AZIONE 4
CO-WORKING
E **CO-DESIGN** PER LA
TRANSIZIONE 4.0 DELLE **PMI**

PARTECIPA

AZIONE 5
PROMOZIONE
E **DIFFUSIONE**
DELLA **MANIFATTURA 4.0**

PARTECIPA

PROGETTO STRATEGICO REGIONALE
MANIFATTUR@ CAMPANIA: INDUSTRIA 4.0

PER MAGGIORI INFO:
https://**manifattura4puntozero**.cittadellascienza.it
manifattura4.0@cittadellascienza.it

POR CAMPANIA FESR 2014-2020

Unione Europea

REGIONE CAMPANIA

FONDAZIONE IDR CITTÀ DELLA SCIENZA