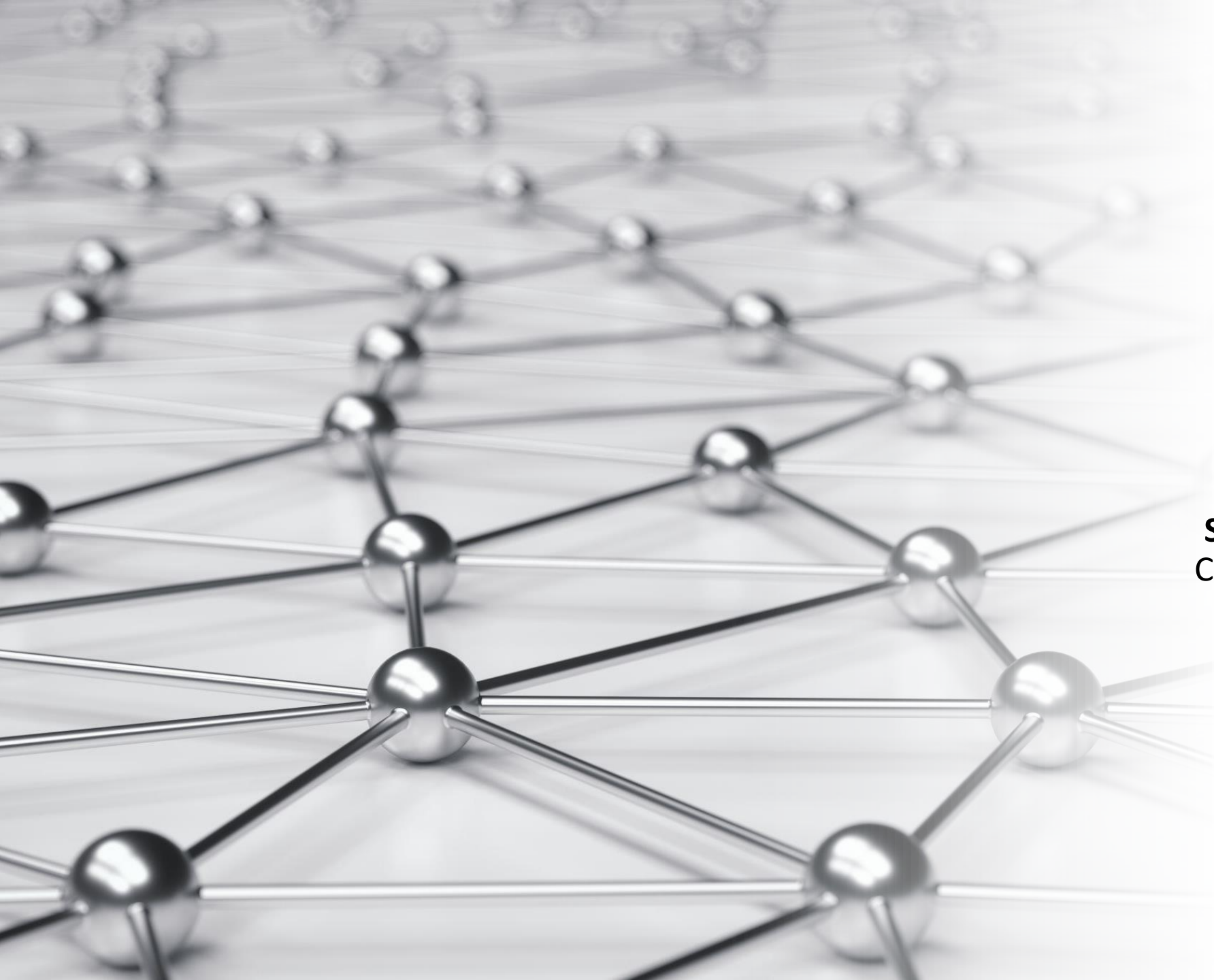
I SERVIZI AVANZATI IN AMBITO CYBERSECURITY DELLA $R^2Lab_{4.0}$ (Rete Regionale dei Laboratori 4.0)

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA



LA VISION

$R^2Lab_{4.0}$ è la rete coordinata da **Fondazione Idis – Città della Scienza**, dei Laboratori di ricerca, Centri di trasferimento tecnologico e altri qualificati Intermediari dell'innovazione che operano in Campania nell'offerta di servizi a supporto dello sviluppo e/o adozione delle tecnologie 4.0 da parte di imprese, cittadini e PA.

LA MISSION

La mission della **R²Lab**$_{4.0}$, è di contribuire alla qualificazione, potenziamento, promozione e valorizzazione dell'offerta di servizi tecnici e di knowledge-intensive a supporto della transizione 4.0 secondo una prospettiva di integrazione partecipata per sfruttare le complementarietà e i vantaggi di un'adeguata massa critica di risorse strumentali e competenze tecniche distribuite e diffuse nel territorio della **Regione Campania**.

La **partecipazione alla rete è aperta**

e avviene mediante richiesta di accreditamento rispetto ad una o più aree tecnologiche abilitanti

VAI AL QUESTIONARIO
ppatura dei provider dei servizi
upporto della transizione 4.0

L'ANALISI DEI FABBISOGNI TECNOLOGICI DELLE PMI

Metodologia Implementata	CAWI - Computer Assisted Web Interviewing
Imprese **contattate** tramite mail	Oltre 650
Imprese contattate mediante telefono	386
Imprese che hanno compilato il questionario	104 (redemption = 27%)

Rischio Cybersecurity: solo 1 su 3 applicano tecnologie e processi adeguati, ma oltre la metà ritiene essenziale collaborare con Provider e figure professionali specializzate in ambito informatico

I rischi

52% Non prevedono nell'organigramma una figura responsabile per implementare processi per la trasformazione digitale

33% Applicano tecnologie, processi e controlli in ambito cybersecurity

13% Hanno certificazione ISO 27001 per la sicurezza delle informazioni

SECURITY RISK ANALYSIS: VULNERABILITY ASSESSMENT E PENETRATION TESTING

SECURITY & PRIVACY COMPLIANCE

I desiderata

78% Le imprese per cui è molto o molto importante collaborare con Provider in grado di trasferire competenze e tecnologie per la cybersecurity

53% Le imprese che prevedono investimenti in investimenti per avviare/potenziare processi di digitalizzazione in R&D

51% Chi reputa necessari gli ingegneri informatici per migliorare l'efficienza in ambito 4.0

POTENZIAMENTO DELLA SECURE NETWORK

IDENTITY & AUTHENTICATION TOOLS PER IL SECURE WEB

L'ANALISI DEI FABBISOGNI TECNOLOGICI DELLE PMI

Boom di cyber attacchi nel 2022

In aumento le imprese anti hacker. Italia a due velocità

Il 94% degli enti ammette di avere avuto un incidente di sicurezza negli ultimi 12 mesi, con l'89% che ammette di essere molto o abbastanza preoccupato per l'impatto della situazione geopolitica

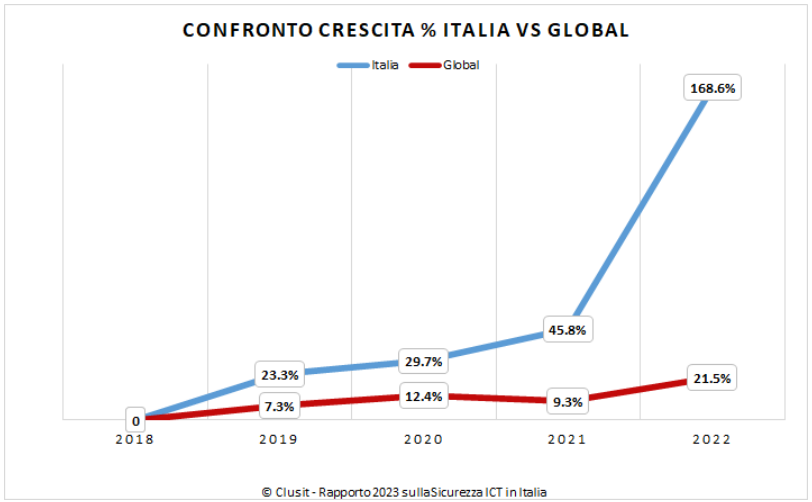
Pagina a cura
DI ANTONIO LONGO

Nel primo semestre del 2022 si sono registrati in Italia 1.572 tra attacchi, incidenti e violazioni della privacy, numero superiore a quelli accaduti nell'intero anno 2021, quando tali casi furono, complessivamente, 1.356. A rivelarlo sono i dati contenuti nel nuovo report stilato dall'Osservatorio Cybersecurity di Exprivia sulle minacce informatiche in base al quale nonostante la cur-

tori più colpiti dalle sanzioni emesse dal garante per la protezione dei dati personali. «Se la leggera diminuzione delle minacce nel secondo trimestre dell'anno da un lato fa presumere una maggiore sicurezza informatica nei servizi digitali che si sono evoluti in questi anni, dall'altro complessivamente il fenomeno del cybercrime continua a mantenere un trend di crescita molto alto» commenta **Domenico Raguseo**, direttore cybersecurity di Exprivia, «per la prima volta, inoltre, l'osservatorio ha elaborato degli indici di calcolo che misurano l'impatto dei dispositivi Internet of Things sulla sicurez-

sistemi individuali che risultano quelli più a rischio, come telecamere di video sorveglianza, stampanti, fino agli stessi programmi antivirus. Al Nord, invece, dove si registra la maggiore diffusione dei dispositivi IoT, dovuta anche alla concentrazione delle industrie, i dispositivi sono più protetti ma i servizi digitali a disposizione dei cittadini sono più esposti a vulnerabilità e presi maggiormente d'assalto dagli hacker.

I settori più colpiti e le motivazioni. Nel secondo trimestre dell'anno corrente, il cybercrime si conferma la motivazio-



Il crescente aumento di attacchi verso PA ed aziende, e la rispondenza agli obblighi di legge imposti dal GDPR ha posto al centro di molti progetti di digitalizzazione la protezione di dati e servizi.

La cybersecurity diventa non più opzionale, ma indispensabile per la business continuity e la prosperità del tessuto produttivo italiano. Le spese dirette e indirette, di un attacco cyber sono in costante crescita. Per il mantenimento delle misure di difesa, le aziende si sono trovate a dover fronteggiare un problema composto da differenti variabili.

Molte PMI non dispongono né di un piano di Disaster Recovery né di Incident Response oltre a non investire sufficientemente in soluzioni di cybersecurity.
Oltre a soluzioni tech in grado di rispondere alle minacce ne servono anche per la cultura del cambiamento e del rischio. Perché l'uomo resta sempre l'anello debole della catena.

I SERVIZI DEL NODO CYBERSECURITY

SERVIZIO	AMBITO APPLICATIVO	TARGET	OUTPUT	PREZZO BASE
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	• PMI operanti nei settori dei servizi avanzati; • PMI operanti nei settori manifatturieri con elevati requisiti di sicurezza; • PA con elevati requisiti di sicurezza.	• Security Awarness e assessment; Stima empirica delle vulnerabilità di un sistema/rete aziendale; • Definizione della strategia e tecnologie da adottare per la mitigazione dei rischi in materia di cybersecurity.	**€ 15.000**
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	• PMI; PA con elevati requisiti di sicurezza	• Conformità relative ai quadri nazionali e internazionali, ai regolamenti obbligatori e agli standard ISO per il settore pubblico e provato; • Sviluppo di soluzioni adeguate alle normative vigenti in tema GDPR	**€ 22.000**
CYBSEC.3 – POTENZIAMENTO DELLA SECURE NETWORK	• Analisi dell'architettura di una rete aziendale esistente ed 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	• PMI operanti nei settori dei servizi avanzati • PMI operanti nei settori manifatturieri con levati requisiti di sicurezza e potenziale rischio di attacco informatico	• Potenziamento dei livelli di sicurezza delle reti aziendali	**€ 24.000**

Settori dei servizi avanzati: salute, trasporti, gestione, manutenzione e monitoraggio delle reti e delle infrastrutture
Settori manifatturieri con levati requisiti di sicurezza e potenziale rischio di attacco informatico: aerospazio, automotive, biotech

I SERVIZI DEL NODO CYBERSECURITY

SERVIZIO	AMBITO APPLICATIVO	TARGET	OUTPUT	PREZZO BASE
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.	• PMI operanti nei settori dei servizi avanzati • PMI operanti nei settori manifatturieri con levati requisiti di sicurezza e potenziale rischio di attacco informatico	• Utilizzo di servizi di autenticazione decentralizzati e innovativi (vedi blockchain, DLT); • Gestione sicura dell'identità degli utenti su sistemi tecnologici in maniera decentralizzata o federata; • Possibilità di definire ruoli e permessi destinati agli utenti nella loro attività su sistemi tecnologici.	€ 23.500
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 blockchaine la loro notarizzazione su tecnologia blockchain.	• PMI operanti nei servizi avanzati (es. salute, trasporti, gestione, manutenzione e monitoraggio delle reti e delle infrastrutture); • PA chiamate a gestire una grande mole di documenti digitali ed elevati requisiti di sicurezza.	• Gestione e archiviazione sicura di documenti digitali con valore legale • Sensibilizzazione verso l'utilizzo di applicazioni decentralizzate basate su blockchain	€ 15.000

Settori dei servizi avanzati: salute, trasporti, gestione, manutenzione e monitoraggio delle reti e delle infrastrutture
Settori manifatturieri con levati requisiti di sicurezza e potenziale rischio di attacco informatico: aerospazio, automotive, biotech