UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO

CONFINDUSTRIA SERVIZI
INNOVATIVI E TECNOLOGICI

ACN
AGENZIA PER LA CYBERSICUREZZA NAZIONALE
SAPIENTIA ADIUVAT

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Posteitaliane

CYBERSECURITYREADINESS.IT

Cyber Security Readiness

Rocco Mammoliti, GT Cybersecurity Unindustria, Poste Italiane

UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA

LUISS

CIS SAPIENZA
RESEARCH CENTER OF CYBER INTELLIGENCE
AND INFORMATION SECURITY

cini
consorzio
interuniversitario
nazionale
per l'informatica

European
DIGITAL SME
Alliance

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

Obiettivi di Cyber Security Readiness

- Supportare e diffondere un **adeguato livello** di **Cyber Security Readiness nelle PMI**
- **Divulgare, formare e sensibilizzare** sulle tematiche rilevanti ed a maggior impatto per il tessuto produttivo nazionale
- Fare leva sulle **Associazioni territoriali e nazionali** che includono PMI e Grandi Aziende per sviluppare e rafforzare la Cybersecurity nella Value-Chain (Sistema Paese)
- Supportare lo sviluppo di un **Ecosistema Efficace**, **Innovativo** e **Resiliente** sulla Cyber Security
- Identificare, supportare e valorizzare le **Eccellenze Italiane** (**Made-In-Italy**) nell'ambito della Cyber Security
- Promuovere una **Comunità Estesa** di esperti (es. *CISO Com.*) con know-how specialistico
- Supportare lo sviluppo di un Ecosistema territoriale/nazionale (con CINI, Università, …) che ha come obiettivo la **Resilienza del Sistema Paese**, Rafforzamento Capacity Building degli Enti coinvolti, etc…

FORMAZIONE & AWARENESS

RESILIENZA

Ecosistemi, RETI e ISAC

Obiettivi di Cyber Security Readiness

Il progetto Cyber Security Readiness mira a valutare, sviluppare e promuovere lo stato di preparazione cyber del tessuto economico e produttivo del Paese, con particolare riferimento alle PMI. Le attività pianificate nel progetto sono basate su **tre pilastri:**

Cyber Security Self Risk Assessment Webinar/Workshop

Lancio di alcune **Survey** per effettuare un'analisi approfondita della postura delle aziende (in particolare delle PMI) nei confronti del rischio ICT e delle minacce cyber. In particolare, l'obiettivo del progetto è quello di **fornire gli strumenti** per valutare il **proprio livello di cyber security readiness** identificando eventuali lacune o punti di miglioramento e, conseguentemente, **aumentare la consapevolezza** e la **capacità di protezione** del patrimonio aziendale.

- ✓**Rilevazione fabbisogni**
- ✓**Portale informativo e di readiness**
- ✓**Webinar/workshop di formazione ad hoc**
- ✓**Rapporto Statistico PMI Cyber readiness**

Censimento delle soluzioni Cyber Security

Censimento delle Start-up/Spin-off/PMI che lavorano ed offrono **prodotti/servizi** in ambito **Cyber Security**. Valutazione del **livello di maturità/ TRL** dei prodotti HW, SW e/o Servizi di sicurezza offerti. Utilizzo di un modello di valutazione generale del livello di maturità. **Pubblicazione White List**, clusterizzazione dei prodotti per ambiti, supporto per **valorizzazione delle soluzioni identificate** e tutela marchi, loghi e IPR

- ✓**Modello di valutazione TRL delle Startup**
- ✓**Creare un MarketPlace (tra PMI Innovative in ambito Cybersecurity e la domanda)**
- ✓**Valorizzazione del Made-In-Italy**

Standard Normative, Certificazioni e Laboratori

Valorizzazione dell'eccellenza italiana nella Cyber Security; identificazione delle migliori competenze, soluzioni e servizi; **mappatura con le esigenze ed i fabbisogni reali dell'industria e degli Enti.** Agevolazione dell'accesso alle realtà locali italiane ad un percorso di accreditamento in linea con **Standard, Certificazioni e Laboratori** (ad es. il **CVCN, il Cyber Security Act ed il Perimetro Nazionale**).

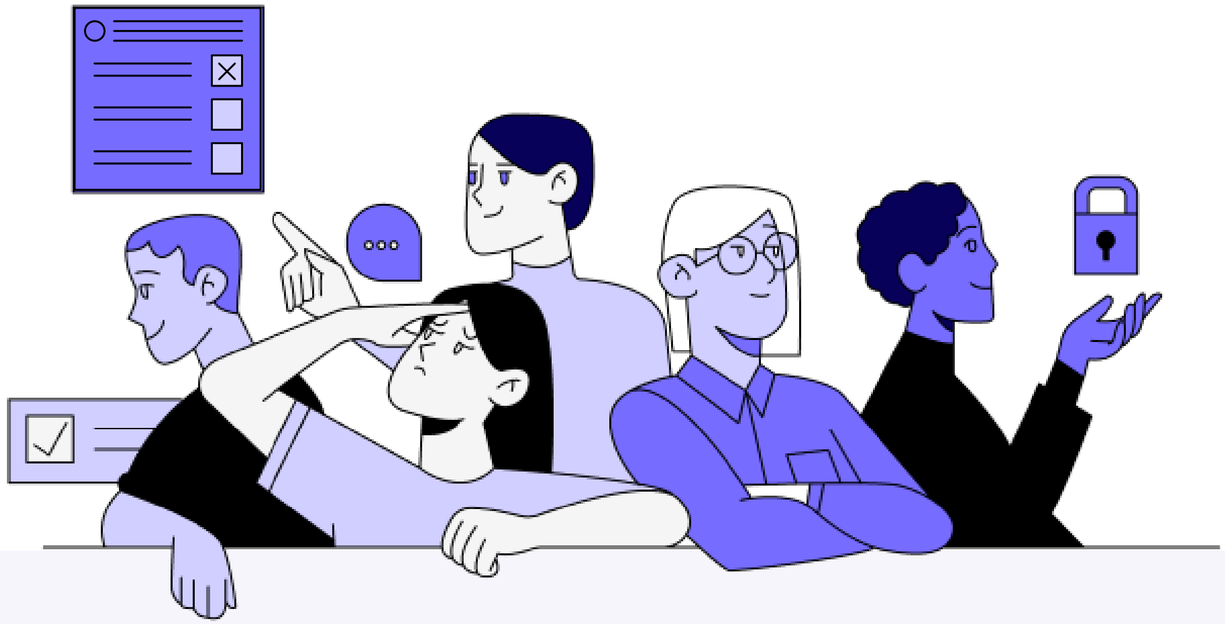
- ✓**Certificazione Tecnica delle Competenze in**
- ✓**Percorsi di certificazione dei prodotti**

CYBERSECURITYREADINESS.IT

Il Portale

CYBERSECURITYREADINESS.IT

Portale online



Il portale **Cyber Security Readiness** ospita servizi e prodotti di facile fruizione per valutare, sviluppare e promuovere lo stato di **preparazione cyber** del tessuto economico e produttivo del Paese, con **particolare riferimento alle PMI**.

CYBER SECURITY SELF RISK ASSESSMENT

ATTIVITÀ DI AWARENESS E FORMAZIONE

STRUMENTI UTILI PER LA SICUREZZA AZIENDALE

CYBERSECURITYREADINESS.IT

Questionari e report

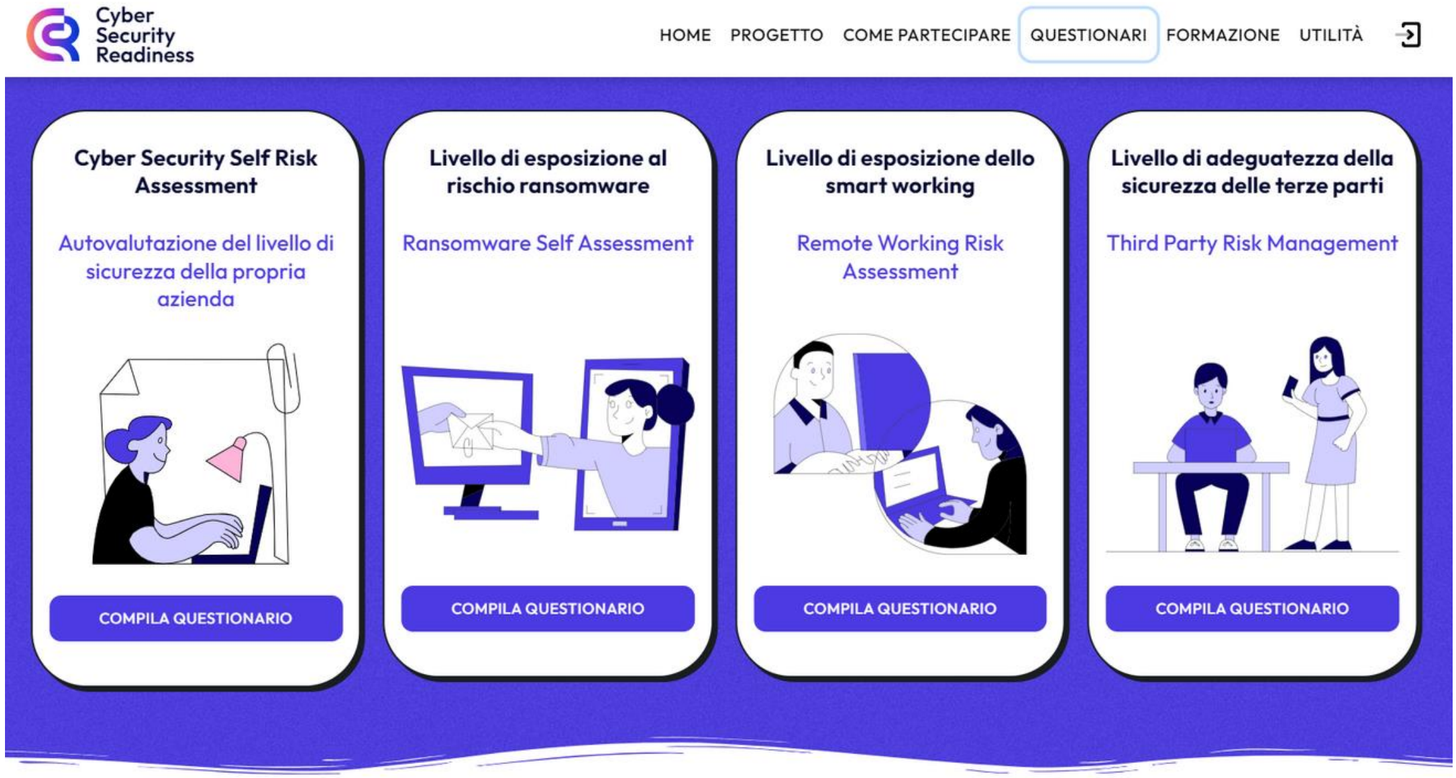
CYBERSECURITYREADINESS.IT

Un questionario per consentire di misurare il proprio **profilo di rischio**, rispetto ad specifici argomenti:

- **Cyber Security Self Risk Assessment**
- **Rischio Ransomware**
- **Smart Working**
- **Terze Parti**

con domande suddivise per dominio di sicurezza:

- GOVERNANCE & ASSET
- SECURITY INFRASTRUCTURE
- PROTEZIONE DEL DATO, BACKUP E DR
- AWARENESS E COMUNICAZIONI
- SECURITY UPDATE E MONITORING
- INFORMAZIONI GENERALI



I questionary 2023

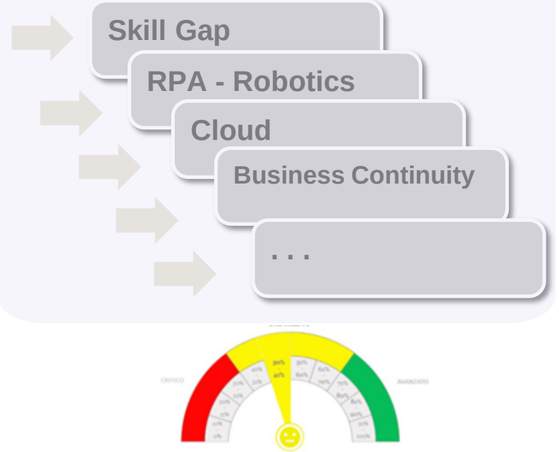
I questionari di **Self-Assesment** rappresentano uno strumento per valutare il livello di maturità rispetto alla Cybersecurity delle PMI ed in generale delle Organizzazioni, allo stesso tempo sono strumenti per **sensibilizzare** e **comunicare** l'importanza di una adeguata gestione della cybersecurity.

METODOLOGIA

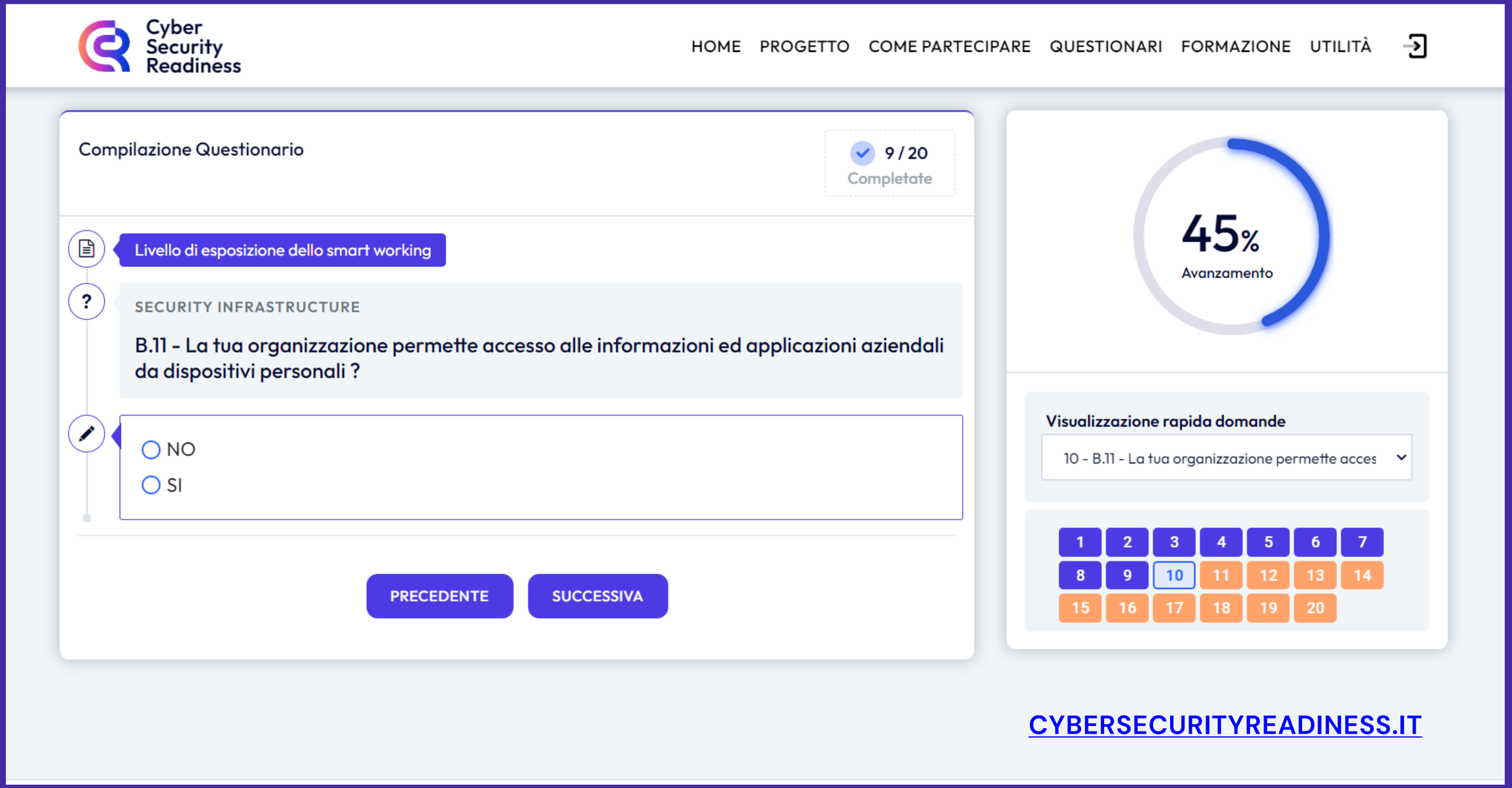
- I questionari affrontano **ambiti specifici**
- Le domande sono distribuite su **6 Domini/Aree**
- Sono restituiti risultati rispetto al **livello di maturità**

- *Veloci*
- *Facili*
- *Anonimi*

Cyber Security Self Risk Assessment		Rischio Ransomware		Smart Working		Terze Parti	
Governance ed Asset	9	Governance ed Asset	9	Governance ed Asset	5	Governance ed Asset	9
Security Infrastructure	8	Security Infrastructure	3	Security Infrastructure	7	Security Infrastructure	9
Protezione del Dato, Backup e DR	5	Protezione del Dato, Backup e DR	3	Protezione del Dato, Backup e DR	-	Protezione del Dato, Backup e DR	5
Security Update e Monitoring.	5	Security Update e Monitoring.	1	Security Update e Monitoring.	1	Security Update e Monitoring.	3
Awarneness e Comunicazioni	3	Awarneness e Comunicazioni	5	Awarneness e Comunicazioni	2	Awarneness e Comunicazioni	2
Informazioni Generali	18	Informazioni Generali	4	Informazioni Generali	5	Informazioni Generali	6



6 Domini
85 Domande


Cyber Security Readiness
HOME PROGETTO COME PARTECIPARE QUESTIONARI FORMAZIONE UTILITÀ
Compilazione Questionario
9 / 20
Completate
Livello di esposizione dello smart working
SECURITY INFRASTRUCTURE
B.11 - La tua organizzazione permette accesso alle informazioni ed applicazioni aziendali da dispositivi personali ?
NO
SI
PRECEDENTE
SUCCESSIVA
45%
Avanzamento
Visualizzazione rapida domande
10 - B.11 - La tua organizzazione permette acces
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20
CYBERSECURITYREADINESS.IT

CYBERSECURITYREADINESS.IT

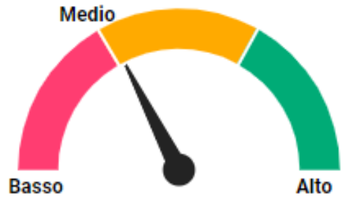
Ogni questionario fornisce un'**analisi dell'esposizione al rischio** della società mediante appositi grafici e alcuni **suggerimenti** per migliorare i propri presidi di sicurezza

STAMPA

Executive Report

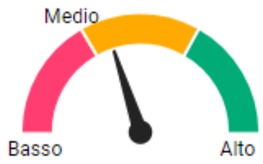
Livello di esposizione al rischio ransomware

Report generato il 30-05-2023 alle ore 11:34



Medio (35.4)

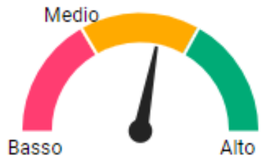
Il tuo cyber index score



40

Awareness e Comunicazioni

La formazione e la sensibilizzazione sulla sicurezza delle informazioni è uno dei processi più imporatanti da implementare per mettere in sicurezza i propri asset, le proprie informazioni. Spesso le Organizzazioni subiscono incidenti che mettono a rischio le informazioni trattate per errori inconsapevoli commessi dai propri dipentenți ed abilmente sfruttati da malintenzionati. Può essere utile ricordare che le Informazioni sono classificate in termini di sicurezza delle informazione anche per livello di criticità e che a livelli di criticità diversi devono seguire normalmente procedure differenti del dato (permessi di accesso, trattamenti, ecc...). I Dipendenti devono conoscere la differeneza di criticità dei dati trattati e l'eventuale rischio che può derivare da un trattamento sbagliato.



55.6

Governance & Asset

Le risposte fornite indicano la possibilità di migliorare i processi le procedure per la protezione del patrimonio informativo dell'Organizzazione, il vero valore di una Organizzazione. L'adozione di Standard di Sicurezza delle Informazioni rappresentano un valido, e spesso necessario, strumento quando si gestiscono informazioni Critiche. Impostare un Framework processi e controlli consente di avere più facilmente il controllo del proprio Livello di Sicurezza, in particolare l'Analisi del Rischio aiuta a determinare le priorità di intervento. Far rivedere il proprio Sistema di Processi e Controlli da professionisti indipendenti può aiutare a migliorarlo.

Protezione del Dato, Backup e DR

Il Report 2023-2024: analisi statistica dei dati e confronto con Report 20-22

Il **Report 2023-2024** avrà una struttura di analisi dei dati che sarà in **continuità con la precedente indagine (2020-2022),** ed offrirà in questo modo un punto di vista aggiornato ed ulteriormente sviluppato su tematiche specifiche (es: smart working, ransomware,…)

La Survey

La Survey si compone di **32 domande** suddivise tra domande **di carattere generale** sull'organizzazione della società **e** domande **di carattere tecnico/organizzativo**.

Le domande di carattere tecnico/specifico si suddividono nelle seguenti macro categorie

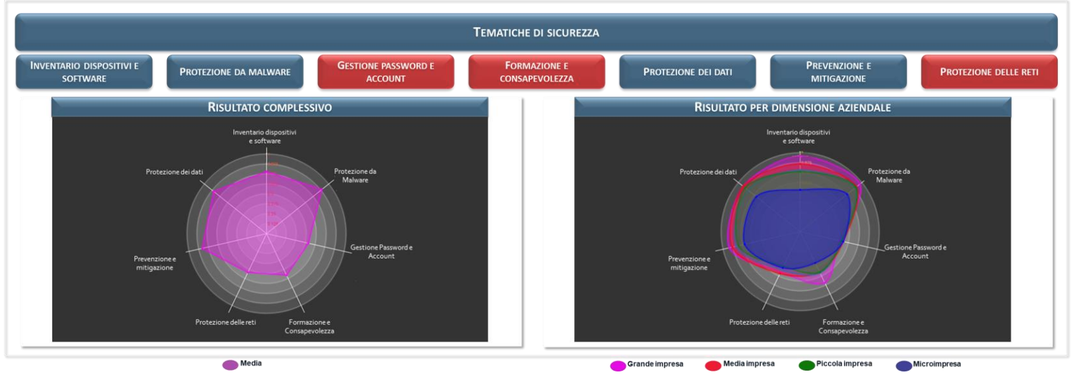
COMMITMENT AZIENDALE
misurare l'attenzione del management in termini di risorse, budget e awareness sulle tematiche di cyber security.

LIVELLO DI ESPOSIZIONE
misurare l'esposizione dell'azienda a minacce/attacchi cyber in funzione della rilevanza servizi/prodotti erogati dall'Azienda

MATURITA' TECNOLOGICA/ORGANIZZATIVA
misurare il grado di maturità tecnologica/organizzativa dell'azienda nel prevenire, contrastare, mitigare le minacce del cyber spazio.

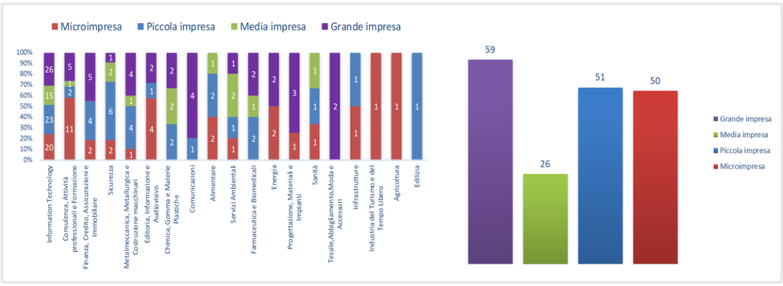
Il Report 2020-2022

Il legame tra Cyber Risk Self Assessment e Controlli Essenziali di Cybersecurity è stato riscontrato in **7 tematiche di sicurezza**



I risultati

186 questionari da aziende appartenenti a diversi settori merceologici e diversificate tra Micro, Piccola, Media e Grande Impresa



- Inventario Dispositivi e Sw
- Protezione Malware
- Gestione Pwd ed Account
- Formazione
- Protezione Dati
- Prevenzione e Mitigazione
- Protezioni Reti

CYBERSECURITYREADINESS.IT

Le Survey sono strumenti che vengono prodotti attraverso l'analisi di specifici contesti e framework di sicurezza.

Lo sforzo e l'attenzione è nel **semplificare la metodologia di indagine** rendendola adeguata al contesto delle PMI e nello sfruttare questo strumento come **veicolo di awareness.**

VANTAGGI:

- ❑ Aggiornamento continuo delle Survey e della Metodologia
- ❑ Estensione dei Domini di Analisi
- ❑ Benefici per le imprese che ricevono un feedback
- ❑ Produzione di Report e statistiche che saranno condivise con ACN, Associazioni e Stakeholder

CYBERSECURITYREADINESS.IT

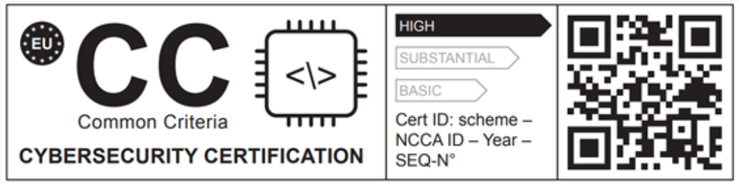
Attività di formazione e awareness

CYBERSECURITYREADINESS.IT

Webinar di Formazione

2023- 2024

TEMATICHE



- Supply Chain Security: sfide ed opportunità per le PMI
- Implementare un programma di Cybersecurity nella propria Organizzazione: Standard, Certificazioni e Gestione del Rischio
- Il Contesto IT/UE in ambito Cybersecurity. Il mercato e le opportunità per le aziende sulla certificazione dei prodotti ICT
- Vulnerabilità e Minacce Cyber: Attacchi informatici e come difendersi
- Nuove Tecnologie Rischi ed Opportunità per le aziende: AI, Wearable, Quantum, Robotics
- CYBER PILLS per le PMI

CYBERSECURITYREADINESS.IT

Webinar di Formazione

1° Evento

6 dicembre 2023

- **Supply Chain Security: sfide ed opportunità per le PMI**

  - ❑ **I - La Supply Chain**
    - Contesto
    - Problemi della S.C. e sfide Globali
    - La compliessità della S.C. – P.o.View: Large Enterprise
    - Rischi e Scenari geopolitici della Supply Chain
  - ❑ **II - Quadro normativo EU/IT sulla cybersecurity della Supply Chain**
    - NIS2
    - DORA/EBA
    - CRA - Cyber Resilience Act
    - GDPR
    - PNSC
  - ❑ **III - Supply Chain Security**
    - Enisa - Good Practices for Supply Chain Cybersecurity
    - Framework Supply Chain Cybersecurity (Nist, …)
  - ❑ **IV - SICUREZZA Terze Parti**
    - Questionario di autovalutazione
    - Strumenti di Cyber Web Reputation (Bitsigth, Security Scorecard, …) – cosa controllano le aziende
    - Audit sulle terze parti
  - ❑ **V - Conclusioni**
    - Incidenti
    - Consigli pratici di readiness / preparazione

CYBERSECURITYREADINESS.IT

Webinar di Formazione

DATE DEL PROGRAMMA

6 Dicembre

25 Gennaio

29 Febbraio

28 Marzo

23 Maggio

20 Giugno

Supply Chain Security: sfide ed opportunità per le PMI

I. La Supply Chain: contesto e sfide globali
II. Quadro normativo EU/IT
III. Supply Chain Security: fotografia dello stato in EU
IV. Standard, Framework e strumenti di monitoraggio
V. Conclusioni

Implementare un programma di Cybersecurity nella propria Organizzazione: Standard, Certificazioni e Gestione del Rischio

I. La Cybersecurity: lo scenario in Italia
II. Standard e Framework di sicurezza: ISO 27001, ISO22301, PNSC, etc.
III. Valutare i Rischi e determinare le opportune contromisure
IV. Modelli Organizzativi: CISO, DPO, CISO As-as-Service
V. Conclusioni

Il Contesto IT/UE in ambito Cybersecurity. Il mercato e le opportunità per le aziende sulla certificazione dei prodotti ICT

I. Contesto EU: sviluppo del Mercato Digitale (DESI)
II. Analisi delle principali Direttive e dei Tavoli di lavoro
III. Certificazione di prodotto
IV. Conclusioni

CYBERSECURITYREADINESS.IT

Webinar di Formazione

DATE DEL PROGRAMMA

6 Dicembre

25 Gennaio

29 Febbraio

28 Marzo

23 Maggio

20 Giugno

Vulnerabilità e Minacce Cyber: Attacchi informatici e come difendersi

I. Evoluzione degli attacchi informatici (scenari geopolitici, hacktivismo, etc…)
II. Tipologie di Attacco e Minacce
III. Ransomware: diffusione e misure di contrasto
IV. Sicurezza comportamentale e social engineering
V. Tecniche e strumenti di IT risk assessment & mitigation
VI. Come difendersi: Misure tecniche di difesa
VII. Conclusioni

Nuove Tecnologie Rischi ed Opportunità per le aziende: AI, Wearable, Quantum, Robotics

I. Mercato Digital & Tech – innovazioni e trend
II. IA Opportunità e punti di attenzione
III. RPA- Robotic Process Automation: Automatizzare i Flussi Aziendali
IV. Sicurezza delle Informazioni e dei Device
V. Conclusioni

CYBER PILLS per le PMI

I. E-mail security (phishing,…)
II. Malicious Software
III. Identità on-line
IV. Smart-working: gestione dei dispositive aziendali
V. Sicurezza mentre si viaggia
VI. Gestione delle Password
VII. ALL overview Vademecum
VIII. conclusioni

CYBERSECURITYREADINESS.IT

Webinar di Formazione

All’interno dei webinar verranno trattati dei Focus tecnologici fortemente richiesti dale PMI associate

- Log Management, Audit, Analysis & Cyber Risk Evaluation – Progettazione, implementazione ed utilizzo di soluzioni Cyber
- Tutela della Proprietà Intellettuale per PMI: sorveglianza e registrazione marchi e loghi, domini, monitoraggio social, patent box, registrazione SW e brevetti
- Cloud, Microservizi, Container, OpenSource: approcci e tools per la sicurezza negli ambienti contenerizzati
- Ciclo di vita del Software: SecDevOps, Processi e soluzioni tecnologiche per la gestione sicura del software
- IA: Opportunità per le PMI, stato dell’arte sui Security Framework, minacce, Etica e sviluppo sostenibile

Il Manifesto Cybersecurity PMI

12 Azioni per rendere sicura la propria Azienda

RISCHIO CYBER

PERCHÉ AUTOVALUTARSI

Scopri gli ambiti specifici in cui è maggiormente esposta la tua organizzazione e le relative pratiche di sicurezza migliori

Domini di sicurezza del QUESTIONARIO

Governance e Asset

Gestione della sicurezza dell'organizzazione con politiche, procedure, standard e certificazioni; controllo delle risorse aziendali attraverso l'inventario degli elementi della catena di valore.

Il raggruppamento delle domande nei principali domini della *cyber security*, ci consente di fornire indicazioni chiare nell'esito finale riguardo gli interventi più urgenti da effettuare per diminuire il proprio livello di esposizione al rischio informatico.

Protezione del dato, Backup e Disaster Recovery

Impiego di soluzioni per la protezione del dato che ne garantiscano riservatezza, integrità e disponibilità in casi di possibili situazioni catastrofiche e di attacchi informatici distruttivi.

Security infrastructure

Adozione di misure di sicurezza per proteggere il patrimonio informativo dell'organizzazione (informazioni classificate o riservate, proprietà industriale, ecc.)

Security update e monitoring

Aggiornamento frequente dei sistemi di sicurezza e monitoraggio costante degli eventi per migliorare la consapevolezza sul proprio livello di esposizione alle minacce informatiche e per consentire interventi di contrasto tempestivi

Awareness e comunicazioni

Sensibilizzazione e formazione del personale per migliorare i presidi di sicurezza aumentando la consapevolezza sugli attacchi informatici e le loro possibili conseguenze

Risorse utili:
- Standard ISO/IEC 27001 per la gestione della sicurezza informatica
- Guida alla cybersicurezza per le piccole e medie imprese - ENISA
- Vademecum Sicurezza Piccole e Medie Imprese – CYBER 4.0

Sicurezza delle terze parti

Collaborare con partner e fornitori per ridurre le vulnerabilità informatiche in modo sistemico

1763 — Attacchi informatici rilevati e contrastati dall'Agenzia per l'Italia Digitale nel 2022

93% — Segnalazioni di campagne malware basate sul tentativo di furto dei dati (personali, professionali e bancari)

50% — Casi in cui si invitano le vittime a prendere visione di falsi ordini e pagamenti

Proteggere i propri sistemi e le informazioni trattate per conto di altre aziende costituisce un elemento fondamentale per la reputazione e il valore di un'impresa.

Allo stesso tempo, assicurarsi che partner e fornitori soddisfino i livelli di sicurezza concordati, estende la protezione aziendale alla catena di approvvigionamento (supply chain) realizzando un modello di difesa collettiva.

- Identificare i rischi cibernetici e i vincoli normativi applicabili sulla base dei prodotti commerciali o servizi erogati
- Valutare e monitorare nel tempo l'esposizione dei partner ad attacchi informatici tramite questionari o audit
- Mappare le relazioni commerciali e tracciare gli accessi ai dati e alle informazioni dell'organizzazione

Risorse utili
- Report ENISA sulle tecniche di attacco rivolte contro la filiera di fornitura
- D.L. 21/09/2019, n. 105 - Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica
- D.P.C.M. 14/04/2021, n. 81 - Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici
- Norma ISO 28000:2007 per la gestione della sicurezza della catena di fornitura
- NIST SP 800-161 Rev. 1 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

PERICOLO RANSOMWARE

Osserva i dettagli prima di agire online

COS'È

È un programma malevolo che:
- **infetta** i dispositivi elettronici (PC, telefoni, ecc.)
- **blocca** l'accesso a ciò che contengono
- **chiede un riscatto** (*ransom*) per tornare alla normalità.

Si diffonde principalmente attraverso **email**, **sms** e **messaggi** provenienti da soggetti apparentemente conosciuti e affidabili oppure navigando su **siti creati o compromessi** dagli hacker.

> Ogni dispositivo infettato ne può contagiare altri, sfruttando la sincronizzazione o accedendo alla rubrica per spedire automaticamente messaggi contenenti il malware.

COME DIFENDERSI

Anche se i messaggi provengono da persone conosciute, controlla sempre la destinazione dei link passandoci sopra il cursore del mouse senza cliccare.
Usa market ufficiali per scaricare le applicazioni e installa software antivirus su tutti i dispositivi.

- **Aggiornamenti regolari**
- **Copia frequente dei dati**
- **Rivolgersi a tecnici specializzati**
- **Denunciare attacchi alla Polizia Postale**
- **Segnalare furto dati al Garante Privacy**

Diffida di inviti allettanti: quasi sempre si tratta di trappole ben congegnate

Per segnalare un attacco, visita il sito NO MORE RANSOM gestito da Europol, polizia olandese, Kaspersky e McAfee

SMART WORKING

Adotta le giuste misure di sicurezza

Il lavoro da remoto espone le aziende a rischi specifici legati all'accesso indesiderato a informazioni di rilievo, anche in modo inconsapevole.

Queste vulnerabilità possono essere mitigate da alcuni interventi basati sulla protezione degli strumenti e sulla formazione del personale coinvolto.

1 Proteggere le comunicazioni su internet, i dispositivi aziendali e quelli personali usati per lavorare da remoto

Indicazioni generali:
- Installa un software antivirus
- Esegui aggiornamenti regolari
- Evita di collegare supporti elettronici senza effettuare una scansione antivirus

Imposta:
- Username e password personalizzati su tutti i dispositivi (no default)
- Codice di accesso per smartphone e tablet
- Salva schermo con codice di sblocco per PC
- Nome della rete Wi-Fi personalizzato
- Firewall sul router
- Crittografia sulla rete
- Log di accesso alla rete

Usa:
- Connessioni sicure (Wi-Fi privato, connessione dati sim aziendale, ecc.)
- Rete privata virtuale (VPN)
- Doppio fattore di autenticazione (strong-authentication)
- Autenticazione biometrica
- Applicazioni autorizzate e verificate

2 Conoscere i comportamenti corretti da assumere per un uso adeguato degli strumenti professionali

Posta elettronica:
- Comunicazioni professionali
- Mittente conosciuto e affidabile
- Scansione antivirus degli allegati
- Filtro antispam
- Log-out al termine dell'attività

Password:
- Diverse per ogni strumento e servizio
- Non condivise
- Lunghe e complesse
- Aggiornate regolarmente
- Sequenze di caratteri imprevedibili
- Generatore e Gestore verificati e attendibili

Navigazione internet:
- Visitare solo siti utili all'attività lavorativa
- Indirizzi web con protocollo https://
- Assicurarsi che l'indirizzo (url) visualizzato nella barra del browser corrisponda al sito che si intende visitare

Risorse utili:
- Strumento SecureHello per generare password robuste
- Servizi di protezione dei sistemi informatici - Cyber 4.0
- Standard ISO/IEC 27033 - Sicurezza della rete

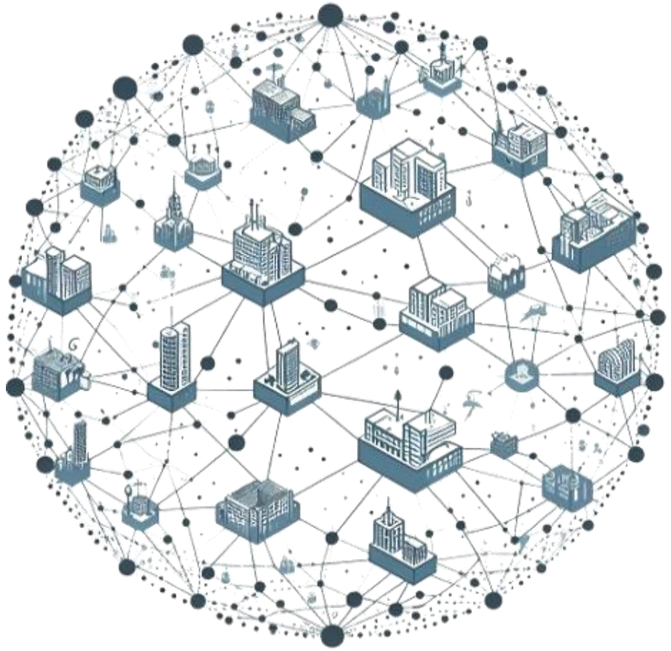
CYBERSECURITYREADINESS.IT

Progetto
Le Terze Parti

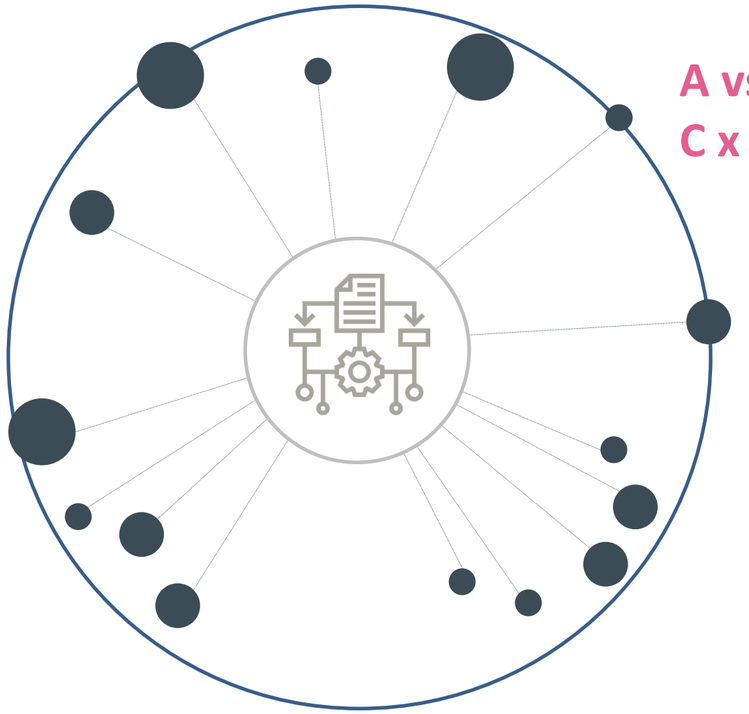
Le Terze Parti: stato dell’arte ed opportunità di migliorare l’ecosistema

Le PMI/SME, oltre 22 Milioni in EU, rappresentano la struttura portante dell’economia comunitaria ed in questo momento sono fortemente coinvolte dalle misure messe in atto dalla Aziende e dall’EU stessa, in termini di **monitoraggio di presidio di degli elementi si sicurezza** e sostenibilità. La strategia è di ottenere una **Supply Chain più Resiliente** e la Supply Chain sta fronteggiando tutto lo sforzo.

A x a x C x S x N



A vs a vs N
C x S



Le PMI sono raggiunte da continue indagini-audit-survey da parte dei loro Clienti rispetto a:

- Survey Cybersecurity / Privacy
- Survey ESG
- Analisi della loro postura internet
- Web reputation
- Audit di seconda pare

❑ Standardizzare il processo di Analisi delle Terze Parti significa:

- Ridurre la complessità ed il carico di lavoro per le PMI
- Migliorare l’efficacia e la veridicità dei processi di controllo
- Poter avere aggiornata una fotografia a Livello Paese sullo stato di salute delle PMI e della Supply Chain

CYBERSECURITYREADINESS.IT

Chi Siamo

Il team

Il prossimo sei tu?

CYBERSECURITYREADINESS.IT

Grazie per l'attenzione.
Vi aspettiamo sul portale.