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

CONFINDUSTRIA SERVIZI
INNOVATIVI E TECNOLOGICI

Posteitaliane

AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

CYBERSECURITYREADINESS.IT

Cyber Security Readiness

Rocco Mammoliti,
GT Cybersecurity Unindustria, Consigliere Sezione IT
Poste Italiane

European
DIGITAL SME
Alliance

UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

CIS SAPIENZA
RESEARCH CENTER OF CYBER INTELLIGENCE
AND INFORMATION SECURITY

cini
consorzio
interuniversitario
nazionale
per l'informatica

LUISS

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

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

Unindustria/CSIT/GLT Cybersecurity

Saluti Istituzionali – VITTORIA CARLI

Saluti e Introduzione al progetto CSR – Cyber Security Readiness –

CSR, Poste Italiane, ROCCO MAMMOLITI

Overview regolamentazione europea in ambito Cybersecurity -

“ Intervento della Commissione europea “ - VITTORIO CALAPRICE

Il sistema Nazionale di Valutazione e Certificazione

Intervento ACN – Agenzia Nazionale Cyber Security – ANDREA BILLET

Le certificazioni di sicurezza dei prodotti ICT: Common Criteria e CEM (Common Evaluation Methodology)

Managing Director ATSEC Information Security - GARIBALDI CONTE

L’Esperienza della ECSO Cyber Security Made in Europe Label

ECSO, CNR, FABIO MARTINELLI

Il Manifesto del Cyber Security Readiness per le PMI

L'obiettivo è Proteggere il Futuro delle PMI

Supportare e diffondere un adeguato livello di **Cyber Security Readiness** nelle PMI (**Formazione**, **Awareness**, **Skills**)

Divulgare, formare e sensibilizzare sulle tematiche rilevanti ed a maggior impatto per il tessuto produttivo nazionale (evoluzione del contesto normativo, certificazioni, etc.)

Supportare lo sviluppo di un **Ecosistema Efficace**, **Innovativo** e **Resiliente** sulla Cyber Security, che ha come obiettivo la **Resilienza del Sistema Paese,** coinvolgimento ed elemento di integrazione tra gli Enti Istituzionali e le PMI

FORMAZIONE & AWARENESS

RESILIENZA
Ecosistemi, RETI e ISAC

I 3 Pillar del CSR:

Cyber Security Self Risk Assessment

Censimento soluzioni / servizi Cyber Made-In-Italy

Matching Domanda/Offerta MarketPlace

Di cosa hanno bisogno le PMI: Serve una guida per gestire la complessità

PSNC-CLOUD
2019-2021

CYBER SECURITY ACT
2021

DATA GOV. ACT
Entrata in vigore: **23.06.2022**
Applicazione: **24.09.2023**

NIS 2/ CER
Entrata in vigore: 16.01.2023
Applicazione: 18.10.2024

eIDAS
DPCM Agid 2024 per passaggio
PEC to REM Eidas 2.0

CYBER SECURITY ACT
17 gennaio 2025

DORA
Applicazione: **17.01.2025**

DATA ACT
Entrata in vigore: **11.01.2024**
Applicazione: **12.9.2025**

IA ACT
Entrata in vigore: **1°sem.24**
Applicazione: **1°sem.26**

Aumenta la difficoltà per le PMI di comprendere ed adattarsi al contesto normativo

Di cosa hanno bisogno le PMI: Serve una guida per gestire la complessità

Cybersecurity	Finance	Trusts & Safety	Data & Privacy	
Regulation for a Cybersecurity Act, (EU) 2019/881 2023/0108(COD)	Common VAT system, (EC) 2006/112, 2022/0407(CNS)	Product Liability Directive (PLD), (EEC) 1985/374, 2022/0302(COD)	European Statistics, (EC) 2009/223, 2023/0237(COD)	Regulation on the free flow of non-personal data, (EU) 2018/1807
Regulation to establish a European Cybersecurity Competence Centre, (EU) 2021/887	Administrative cooperation in the field of taxation, (EU) 2011/16	Toys Regulation, (EC) 2009/48, 2023/0290(COD)	General Data Protection Regulation (GDPR), (EU) 2016/679	Open Data Directive (PSI), (EU) 2019/1024
NIS 2 Directive, (EU) 2022/2555	Payment Service Directive 2 (PSD2), (EU) 2015/2366 2023/0209(COD)	European Standardization Regulation, (EU) 2012/1025	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU) 2018/1725	Data Governance Act (DGA Regulation), (EU) 2022/868
Information Security Regulation, 2022/0084(COD)	Digital Operational Resilience Act (DORA Regulation), (EU) 2022/2554	eIDAS Regulation, (EU) 2014/910, 2021/0136(COD)	ePrivacy Regulation, 2017/0003(COD)	Regulation on data collection for short-term rental, 2022/0358(COD)
Cybersecurity Regulation, 2022/0085(COD)	Crypto-assets Regulation (MiCA), (EU) 2023/1114	Radio Equipment Directive (RED), (EU) 2014/53	European Data Act (Regulation), 2022/0047(COD)	Interoperable Europe Act, 2022/0379(COD)
Cyber Resilience Act, 2022/0272(COD)	Financial Data Access Regulation, 2023/0205 (COD)	Regulation for a Single Digital Gateway, (EU) 2018/1724	European Health Data Space (Regulation), 2022/0140(COD)	Harmonization of GDPR enforcement 2023/0202(COD)
Cyber Solidarity Act (Regulation), 2023/0109(COD)	Payment Services Regulation, 2023/0210(COD)	General Product Safety Regulation, (EU) 2023/988	Access to vehicle data, functions and resources Right to repair Directive, 2023/0083(COD)	GreenData4all
	Digital euro, 2023/0212 (COD)	Machinery Regulation, (EU) 2023/1230		
	Regulation on combating late payment, 2023/0323 (COD)	AI Act (Regulation), 2021/0106(COD)		
		Eco-design Regulation, 2022/0095(COD)		
		AI Liability Directive, 2022/0303(COD)		
		Corporate Sustainability Due Diligence and amending Directive (EU) 2022/0051(COD)		

Legenda

In vigore

In negoziazione

In pianificazione

https://www.bruegel.org

Aumenta la difficoltà per le PMI di comprendere ed adattarsi al contesto normativo

Cosa abbiamo fatto, cosa stiamo facendo

Team di esperti sulla Cybersecurity (*Aziende, Accademia, Associazioni*)

Campagna di Cyber Security Readiness

Metodologia per l'analisi dei prodotti Security Made in ITA

Survey specifiche di rilevamento maturità delle PMI in ambito Cybersecurity su rischi specifici

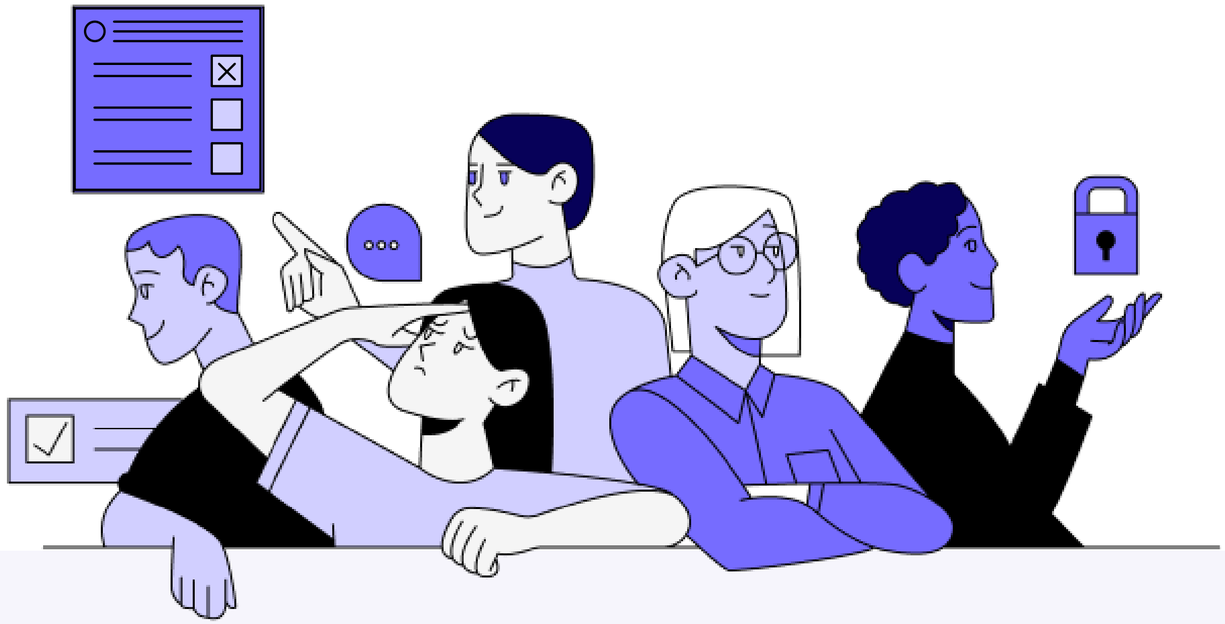
Workshop di formazione per PMI 2023-2024: +6 Eventi

Lancio Portale con Materiale divulgativo

Report statistico finale

Portale online

CYBERSECURITYREADINESS.IT



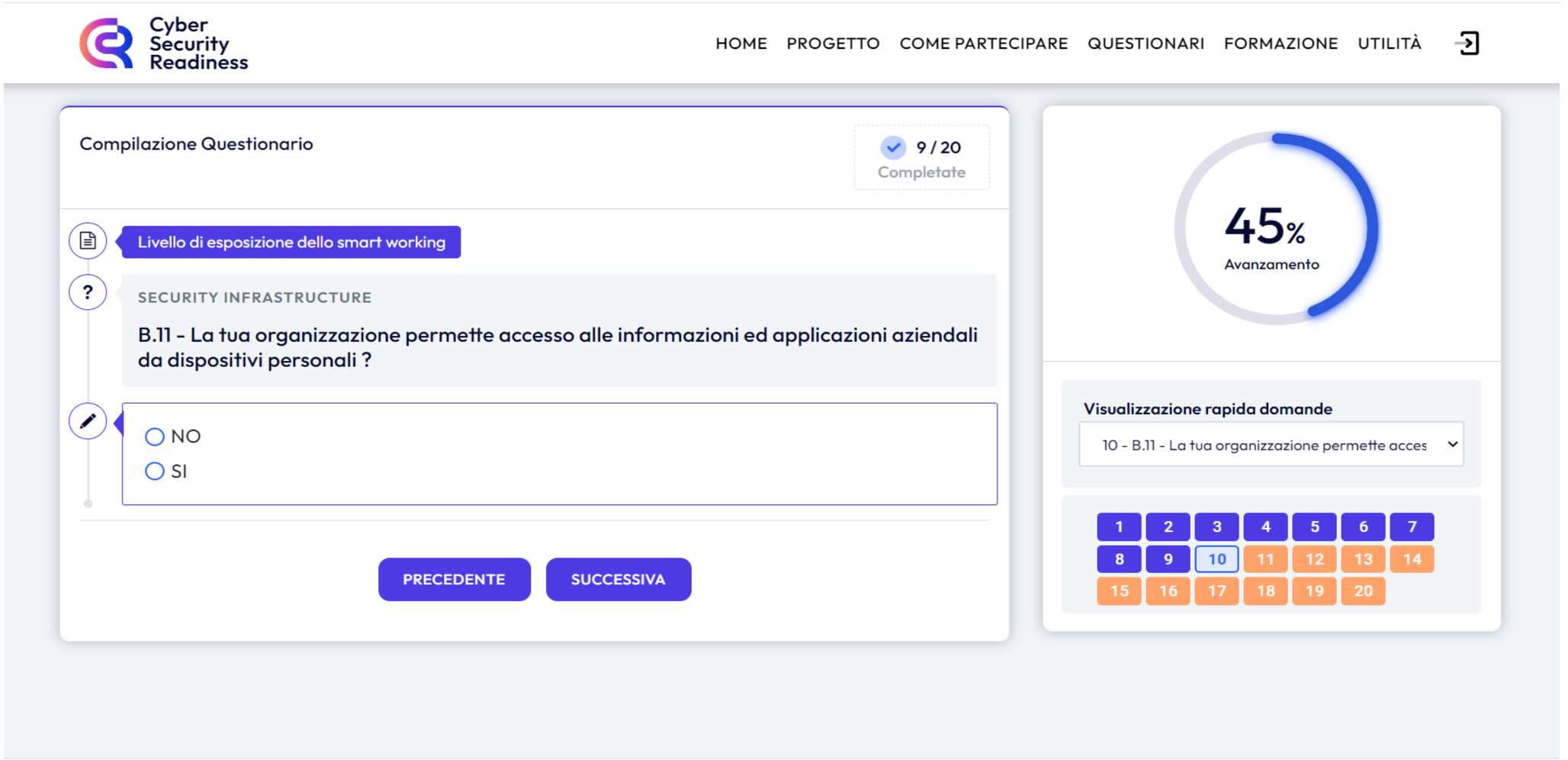
Il portale **Cyber Security Readiness** ospita servizi e prodotti di facile fruizione per valutare, sviluppare e promuovere lo stato di **preparazione cyber** del tessuto economico e produttivo del Paese, con particolare riferimento alle PMI.

CYBER SECURITY SELF RISK ASSESSMENT

STRUMENTI UTILI PER LA SICUREZZA AZIENDALE

ATTIVITÀ DI AWARENESS E FORMAZIONE

Portale online



Portale online

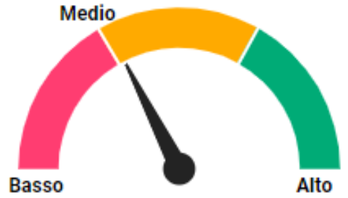
Ogni questionario fornisce un'**analisi dell'esposizione al rischio** della società mediante appositi grafici e alcuni **suggerimenti** per migliorare i propri presidi di sicurezza

STAMPA

Executive Report

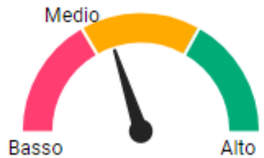
Livello di esposizione al rischio ransomware

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



Medio (35.4)

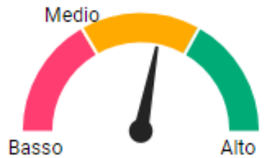
Il tuo cyber index score



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.

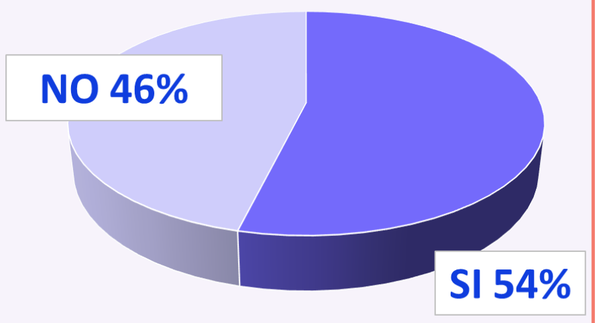
Protezione del Dato, Backup e DR

Le Survey: i primi risultati

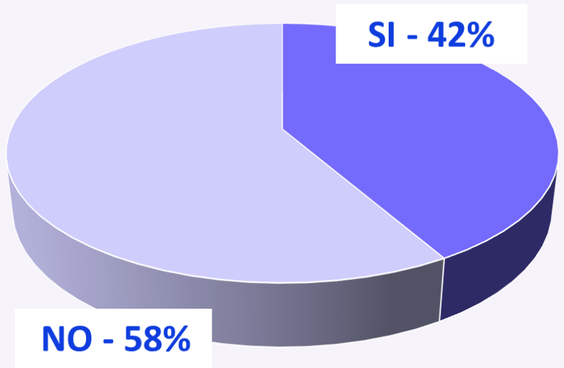
Numero questionari fatti	70	23	27	26
Numero domande per questionario	48	25	20	34
Numero di PMI che hanno risposto al questionario	> 140			
Interesse per la Cybersecurity ? E' fonte di preoccupazione	Si per > 90%			

Le Survey: i primi risultati 2024

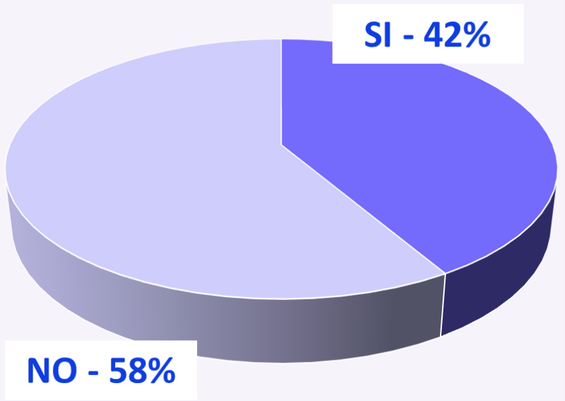
Impiego di SOC (security Operation Center) ?



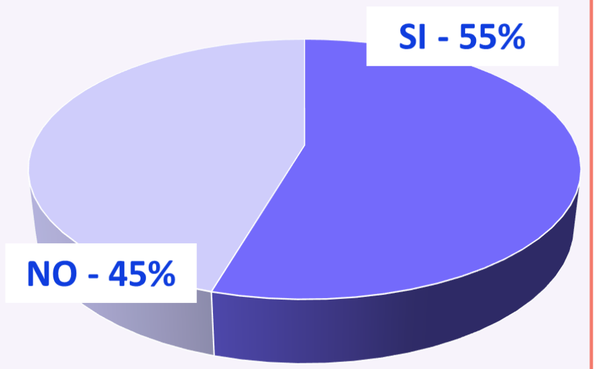
Accesso 2FA ?



certificazioni di Sicurezza – ISO 27001 ?



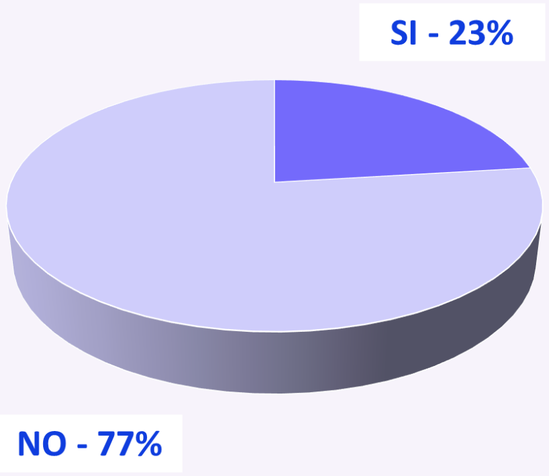
Data Masking e Data Encryption?



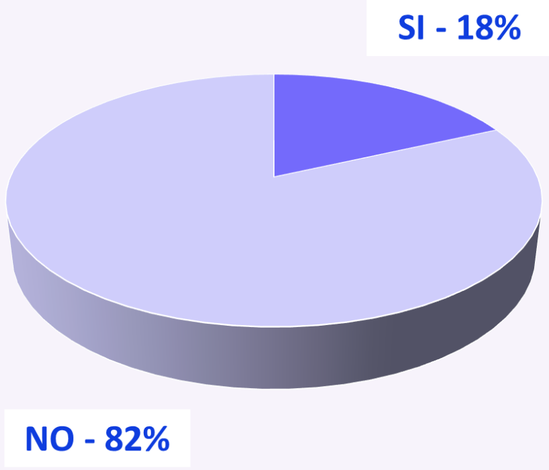
E’ necessario far comprendere l’importanza di gestire la CyberSecurity con strumenti adeguati

Le Survey: i primi risultati

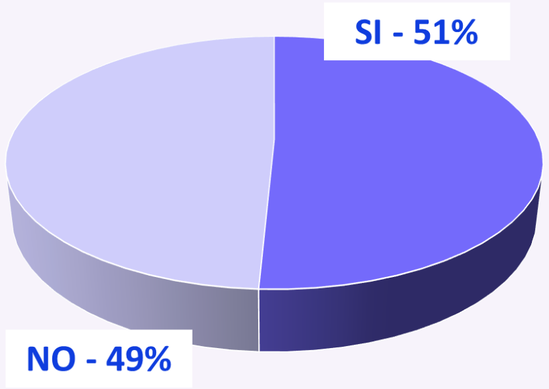
attacchi informatici?



piano protezione Ransomware?



Risk Management ?



Una fotografia che può far pensare che eventuali rischi-eventi possano non essere individuati dalle PMI

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

Il Manifesto Cybersecurity PMI

12 Azioni per rendere sicura la propria Azienda

Piano di Formazione ed Awareness 2023-2024

Workshop di Formazione

2023- 2024

PROSSIMI

- Attacchi Informatici: come difendersi
- Nuove Tecnologie ed opportunità
- Strumenti per la Cybersecurity

Supply Chain Security: sfide ed opportunità per le PMI

I. Introduzione Strategia Cybersecurity Nazionale
II. Supply Chain Security: sfide ed opportunità per le PMI
III. Analisi dei requisiti presenti nei capitolati di gara in tema di Cyber Security
IV. Cyber 4.0 a supporto delle PMI

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

I. Certificazioni accreditate di Sicurezza Informatica
II. Framework Nazionale Cyber Security applicazioni alle PMI
III. GDPR, Data Protection e adempimenti Privacy per una PMI
IV. ISO27001: esempi reali di un Sistema di Gestione
V. Introduzione generale al concetto di RISCHIO e standard di gestione

Focus

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

I. Introduzione: importanza delle certificazioni di Prodotto
II. Contesto Normativo ITA ed EU (Cyber Security Act, Market Place ACN, …)
III. Opportunità di Business e Mercato
IV. Processi di Certificazioni in ambito LaP-CVCN
V. Processo di Certificazione in ambito Cyber Security Act-EU

Chi siamo












- **Rocco Mammoliti**, CISO Poste Italiane
- **Roberto Setola**, Unicampus, Professor and Director Homeland Security
- **Aniello Gentile**, Cyber Security Expert / Board Member of Gaia-X
- **Marco Pinzaglia**, Cyber Security Expert
- **Luigi Martino**, PhD Professor Cybersecurity
- **Vittoria Carli**, Presidente IT Unindustia, Vicepresidente Confindustria,
- **Luca Faramondi**, Assistant Professor Unicampus
- **Massimiliano Cannata**, giornalista
- **Massimiliano Aschi**, Cyber Security Expert
- **Simona Quinzi**, Direttore Confindustria servizi innovativi
- **Marco Angelini**, Assistant Professor, Cyber Intelligence Research
- **Matteo Lucchetti**, Director Cyber 4.0

CYBERSECURITYREADINESS.IT

Grazie per l'attenzione.