FORUM CYBER 4.0

CYBERSECURITYREADINESS.IT

Cyber Security Readiness

Rocco Mammoliti, GT Cybersecurity Unindustria, Poste Italiane

AGENZIA PER LA CYBERSICUREZZA NAZIONALE · ACN · SAPIENTIA ADIUVAT

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

UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA

CIS SAPIENZA
RESEARCH CENTER OF CYBER INTELLIGENCE AND INFORMATION SECURITY

cini consorzio interuniversitario nazionale per l'informatica

European DIGITAL SME Alliance

Posteitaliane

LUISS

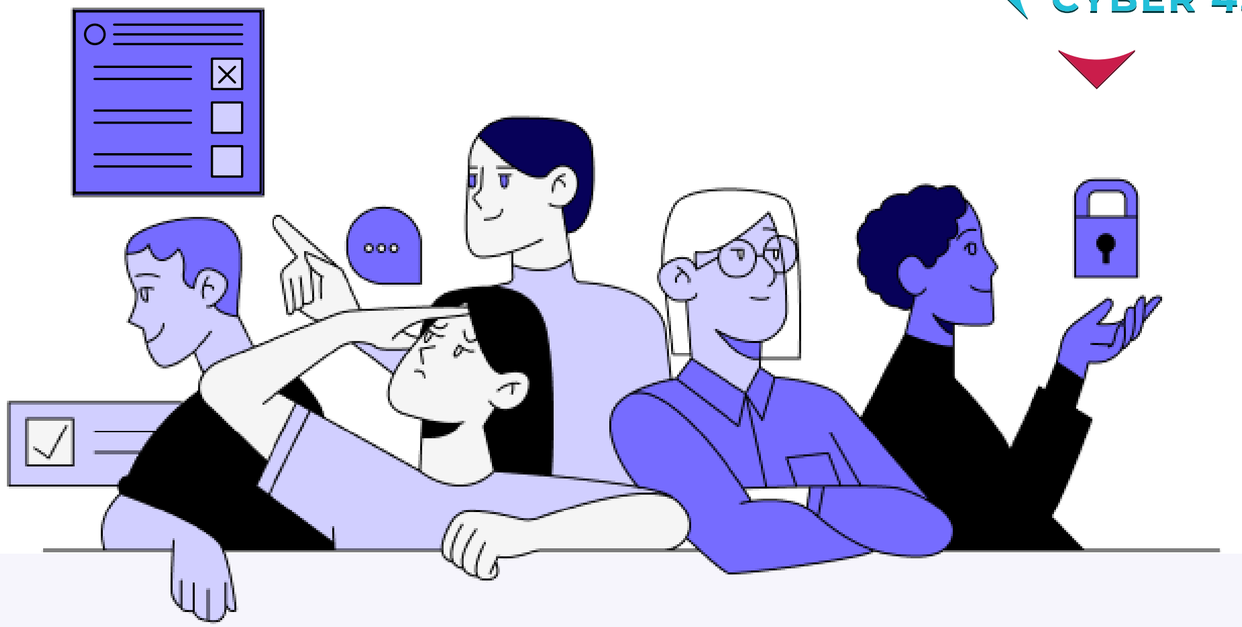
CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

CYBERSECURITYREADINESS.IT

FORUM CYBER 4.0

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 2023

STRUMENTI UTILI PER LA SICUREZZA AZIENDALE

ATTIVITÀ DI AWARENESS E FORMAZIONE

FORUM CYBER 4.0

CYBERSECURITYREADINESS.IT

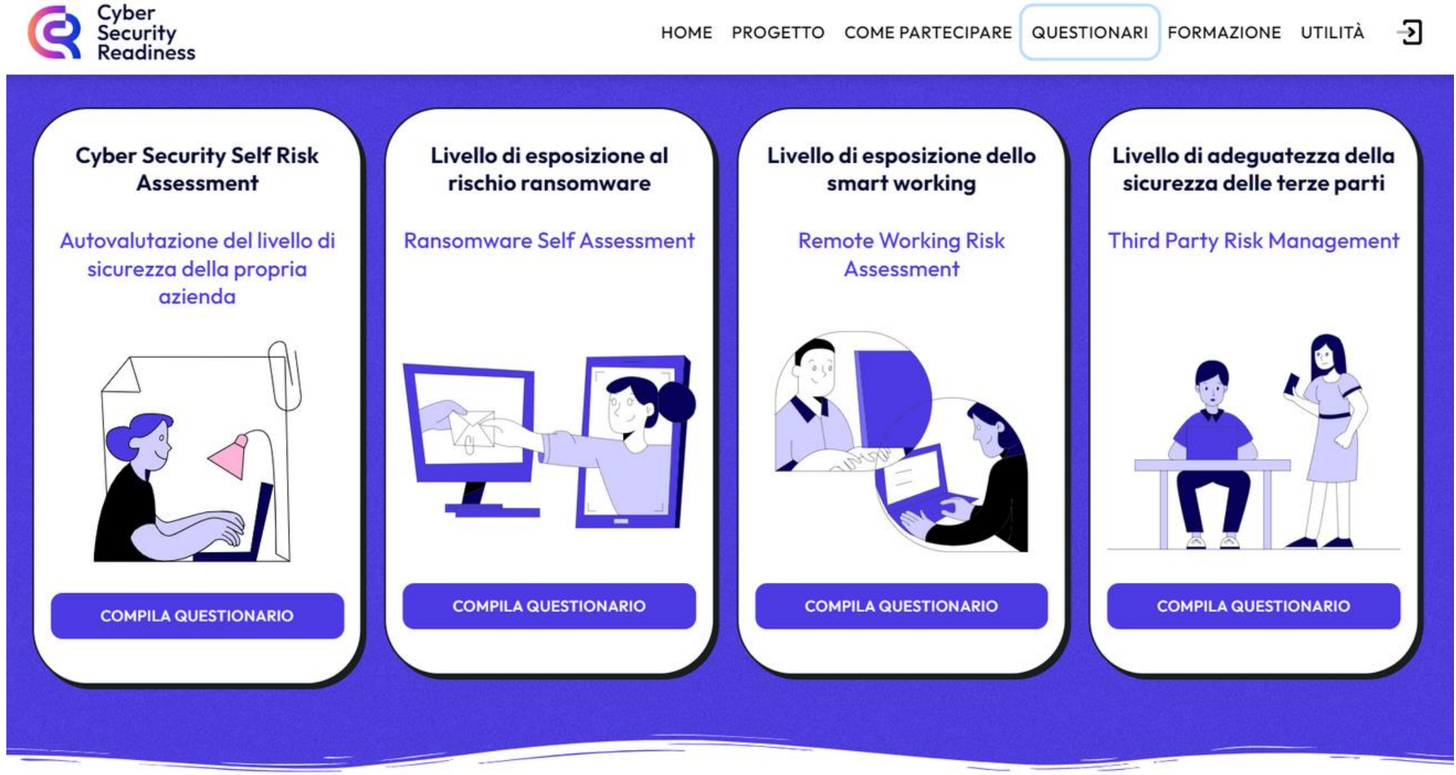
Questionari e report

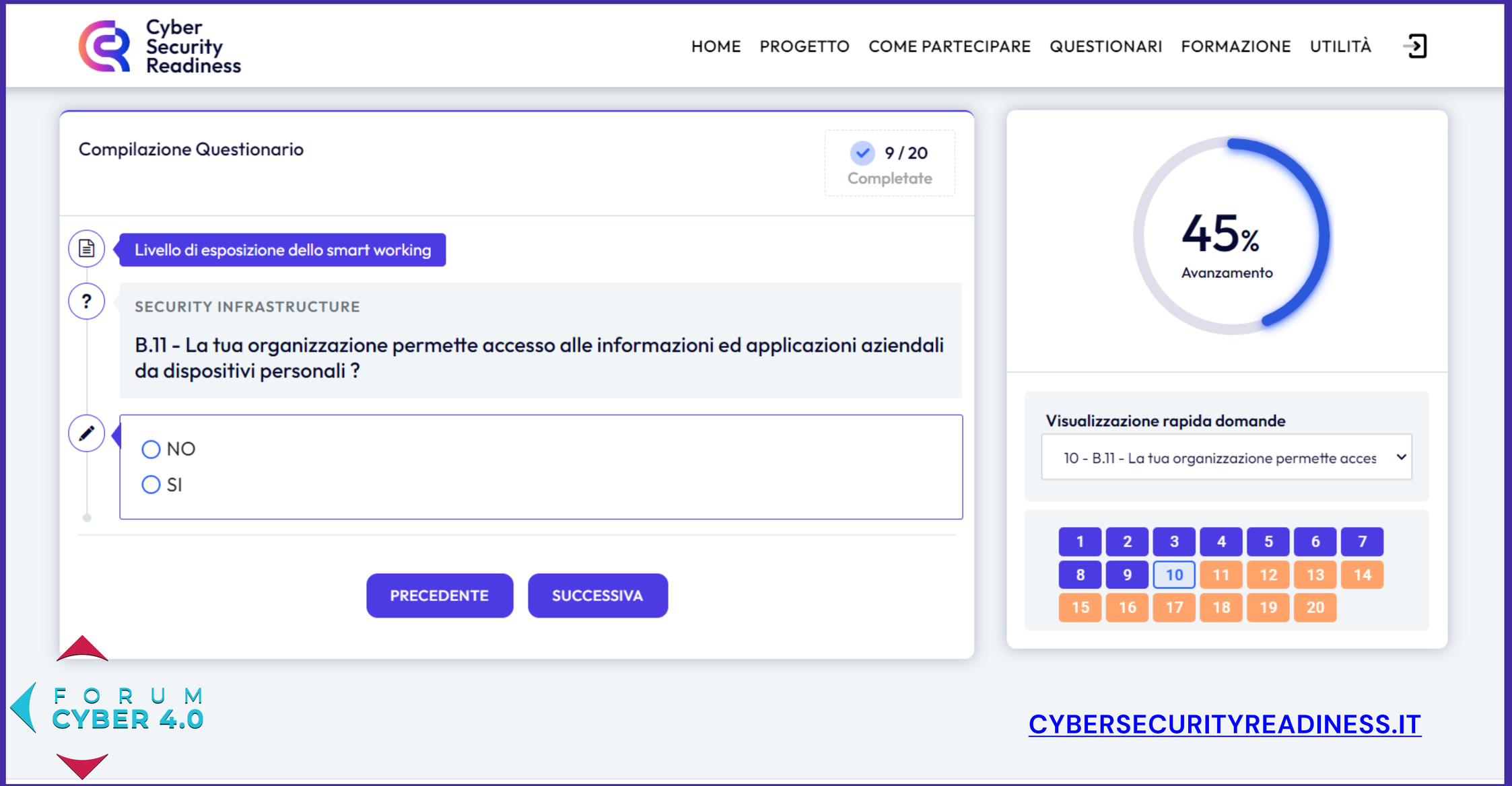
CYBERSECURITYREADINESS.IT

Un questionario per ogni specifico **profilo di rischio**, 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

FORUM CYBER 4.0




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
FORUM CYBER 4.0
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

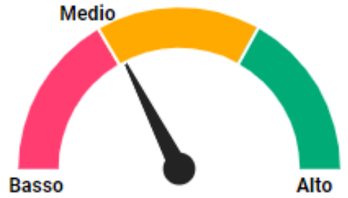
FORUM CYBER 4.0

STAMPA

Executive Report

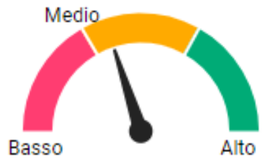
Livello di esposizione al rischio ransomware

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



Medio (35.4)

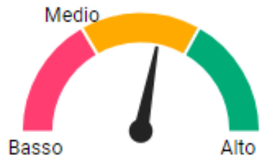
Il tuo cyber index score



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

FORUM CYBER 4.0

CYBERSECURITYREADINESS.IT

Strumenti utili per la sicurezza

CYBERSECURITYREADINESS.IT

FORUM CYBER 4.0

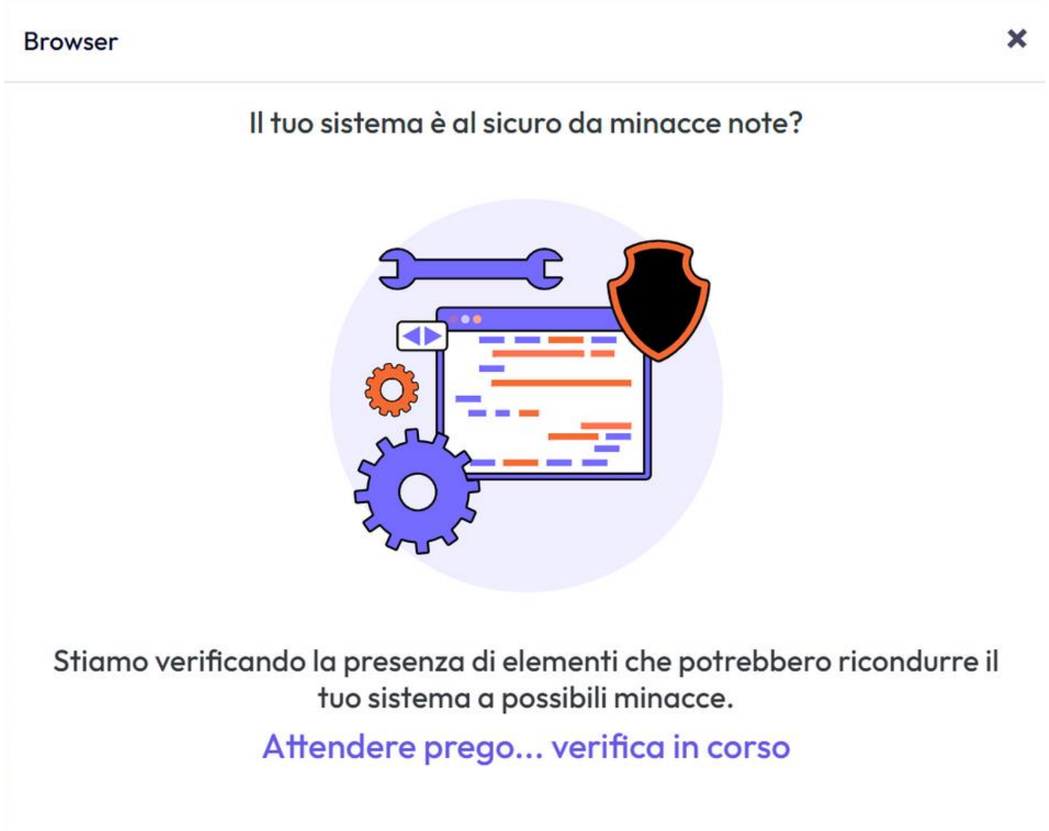
Password check

Assistente artificiale intelligente

- GENERATORE DI PASSWORD COMPLESSE
- CONTROLLO E ANALISI DI CRACKING DELLA PASSWORD INSERITA
- SIMULAZIONE ATTACCO SOCIAL ENGINEERING

CYBERSECURITYREADINESS.IT

FORUM CYBER 4.0



Check vulnerability

Controllo di sicurezza del sistema

- VERIFICA AGGIORNAMENTO BROWSER
- CONTROLLO IP NELLE BLACKLIST DI MALWARE

FORUM CYBER 4.0

CYBERSECURITYREADINESS.IT

Attività di awareness e formazione

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.

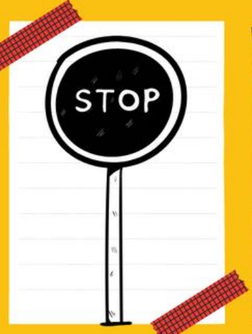
Si diffonde principalmente attraverso **email**, **sms** e **messaggi** provenienti da soggetti apparentemente conosciuti e affidabili oppure navigando su **siti creati o compromessi** dagli hacker.

> 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

Workshop di formazione

- **Laboratori di certificazione dei prodotti e standard Common Criteria**
  Percorsi di certificazione di sicurezza di prodotti: opportunità e qualificazione
- **Ransomware Readiness Assessment**
  Conoscere la minaccia per una migliore prevenzione
- **Livello di Esposizione dello Smart Working**
  Come cambia il profilo della minaccia ed i livelli di Rischio delle Organizzazioni
- **Livello di adeguatezza della Sicurezza delle Terze Parti**
  Vincoli ed opportunità per le PMI di certificazione e conformità di sicurezza
- **Certificazione ISO27001 e Laboratori di VA standard Accredia**
  Cybersecurity e protezione dati: il ruolo della certificazione accreditata
- **ISAC – Information Security Analysis Centre**
  Organizzazione, servizi e sviluppo

FORUM CYBER 4.0

Roadmap delle attività

Il progetto è strutturato in specifiche attività pianificate nel corso dell'anno, che prevederanno il coinvolgimento di **Associazioni**, **Enti** e **Istituzioni** anche nell'ambito del progetto **Polis** di Poste Italiane

Evento Associativo di **Lancio** della Cyber Security Readiness

Campagna di Cyber Security Readiness (tramite Linkedin e social network)

Workshop di formazione utile e **awareness** su Cyber Security Readiness

Periodo di **rilevazione** (Giugno-Settembre 2023)

Analisi ed **elaborazione** dati (Settembre-Ottobre 2023)

Predisposizione **Report 2023** (Ottobre 2023)

Evento di **pubblicazione** dei **risultati** (Ottobre-Dicembre 2023)

Prossimi passi

FORUM CYBER 4.0

LANCIO SURVEY CYBER SECURITY READINESS

IMPLEMENTAZIONE CENSIMENTO E VALUTAZIONE MATURITÀ DELLE SOLUZIONI CYBER SECURITY

APPROFONDIMENTI SU CVCN/LAP E LABORATORI ACCREDITATI (FOCUS CON ACCREDIA, ACN)

ANALISI E CONDIVISIONE RISULTATI SU STANDARD, NORMATIVE, CERTIFICAZIONI E LABORATORI

SURVEY SPECIALISTICA SU RISCHI E OPPORTUNITÀ DEL **CLOUD**

SURVEY SPECIALISTICA SULLA **RESILIENZA/ CONTINUITÀ OPERATIVA** A FRONTE DI SCENARI DI CRISI

CYBERSECURITYREADINESS.IT

Grazie per l'attenzione.
Vi aspettiamo sul portale.

FORUM CYBER 4.0