FORUM CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

FORUM
CYBER 4.0

Vademecum PMI
12 passi per un business più sicuro

Martina castiglioni

RESPONSABILE FORMAZIONE E ADVISORY,
CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Cyber 4.0 a supporto delle PMI

Attività istituzionali | Servizi di mercato | Progetti finanziati | Networking

Orientamento PMI

Vademecum PMI

- **12 azioni** per un business sicuro
- Basato su 12 Step ENISA

Ministero delle Imprese e del Made in Italy

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

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

Postura cyber security PMI

- Basato su **Framework Nazionale Cybersecurity e Data Protection**
- **Analisi** aree di intervento prioritario, remediation roadmap, impatto economico e benefici
- **Estensione nazionale** – DIH, PID, Case Tecnologie Emergenti

Roadshow Cyber 4.0

- Coinvolgimento DIH e altre realtà attive in regione (Polizia Postale, CTE, etc.)
- Sessioni di info/ formazione e incontri con esperti, case studies e buone pratiche, quick Cyber Checkup
- Aggregazione di comunità locali per **information sharing**

FORUM CYBER 4.0

Introduzione al VADEMECUM - Il contesto di riferimento

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

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Ministero delle Imprese e del Made in Italy

I 12 passi

1. *Sviluppare una solida cultura della cybersicurezza*
2. *Fornire una formazione appropiata*
3. *Garantire un’efficace gestione dei terzi*
4. *Sviluppare un piano di risposta agli incidenti*
5. *Rendere sicuro l’accesso ai sistemi*
6. *Rendere sicuri i dispositivi*
7. *Rendere sicura la propria rete*
8. *Migliorare la sicurezza fisica*
9. *Rendere sicuri i back up*
10. *Lavorare con il cloud*
11. *Rendere sicuri i siti online*
12. *Cercare e condividere conoscenze ed informazioni*

Introduzione al VADEMECUM - Il contenuto

Titolo

Azione

Integrazione

- ***Contesto e parole chiave (glossario)***
- ***Raccomandazioni***
- ***Riferimenti al contesto nazionale***
- ***Riferimenti metodologici***

Esempio

4. Sviluppare un piano di risposta degli incidenti

Testo originale di ENISA

- **Parole chiave** – Incidente informatico, Data Breach, IoC, Polizia Postale, CSIRT Italia, High impact Incident.
- **Raccomandazioni** – Come creare un piano di risposta degli incidenti? Fasi: attività, ruoli, tempistiche – pianificazione e preparazione, identificazione e valutazione dell'evento, gestione, notifiche, miglioramento continuo)
- **Riferimenti nazionali** – Quando e come notificare un incidente informatico
- **Methodological references**
  - Riferimenti legislativi nazionali ed europei (NIS, NIS2, D.Lgs 65/2018, PSNC)
  - Riferimenti ai meccanismi di notifica nazionali
  - FNCS (Framework Nazionale per la Cybersecurity e la Data Protection)
  - Altri framework per la gestione degli incidenti

Introduzione al VADEMECUM - Il contenuto

Titolo

Azione

Integrazione

- ***Contesto e parole chiave (glossario)***
- ***Raccomandazioni***
- ***Riferimenti al contesto nazionale***
- ***Riferimenti metodologici***

Esempio

6. Rendere sicuri i dispositivi

- **Mantenere il software corretto ed aggiornato**
- **Anti-virus**
- **Utilizzare strumenti di protezione per i messaggi di posta elettronica ed il web**
- **Crittografia**
- **Attuare la gestione dei dispositivi mobili**

Testo originale di ENISA

- **Parole chiave** – Patch, VAPT, VIRUS, Incidente informatico, Data Breach, IoC, Polizia Postale, CSIRT Italia, High impact Incident.
- **Raccomandazioni** – come scegliere l'antivirus, come riconoscere il phishing, consigli per l'utilizzo sicuro della posta elettronica, utilizzo della VPN, utilizzo di reti WIFI.
- **Riferimenti nazionali** – FNCS (Framework Nazionale per la Cybersecurity e la Data Protection)

Introduzione al VADEMECUM - Il contenuto

Titolo

Azione

Integrazione

- ***Contesto e parole chiave (glossario)***
- ***Raccomandazioni***
- ***Riferimenti al contesto nazionale***
- ***Riferimenti metodologici***

Esempio

11. Rendere sicuri i siti on-line

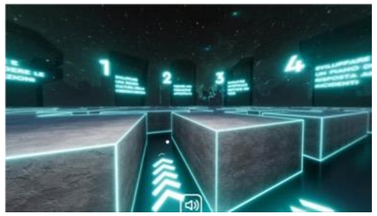
Testo originale di ENISA

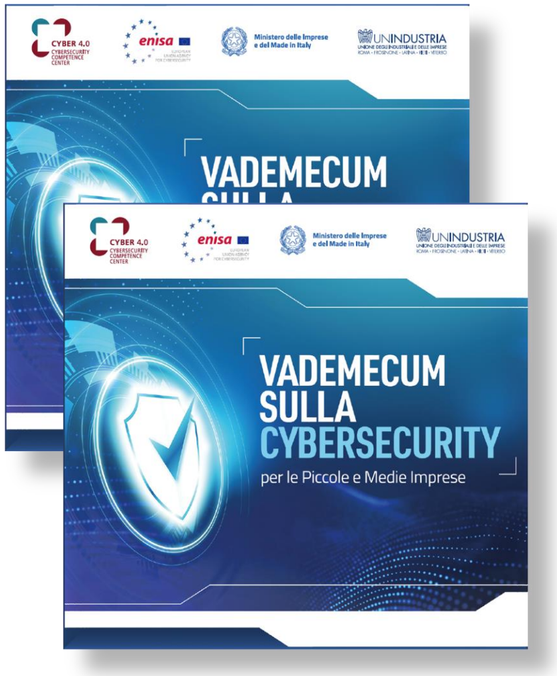
- **Raccomandazioni** – utilizzo della connessione HTTPS, gestione dei cookies, gestione dei dati personali per gli utenti dei siti web, come utilizzare un Content Management System in maniera sicura.

- **Riferimenti nazionali** – FNCS (Framework Nazionale per la Cybersecurity e la Data Protection), normativa e linee guida in merito alla gestione dei cookie, riferimenti alla normativa privacy.

Prossimi passi

- *T4*





- *Formazione e consapevolezza*
- *Cybersecurity assessment*

- *Roadshow Cyber 4.0*