SPECIALE 2025

VOL. 01

CYBER SECURITY IN AZIENDA

30 STRATEGIE

formato
E-BOOK

tnsolutions.it

CYBER SECURITY IN AZIENDA

30 STRATEGIE

01

Gestione delle Password

- Utilizzo di password complesse e uniche.
- Implementazione di un gestore di password aziendale.
- Periodico aggiornamento delle password.

02

Autenticazione Multi-Fattore (MFA)

- Obbligo di MFA per l'accesso ai sistemi critici.
- Utilizzo di app di autenticazione o token fisici per MFA.

03

Aggiornamento e Patch di Software

- Controllo e applicazione regolare delle patch di sicurezza.
- Mantenere tutti i sistemi operativi e software aggiornati.

04

Antivirus e Antimalware

- Installazione e aggiornamento regolare di software antivirus e antimalware.
- Scansioni di sicurezza periodiche.

05

Firewall Avanzato

- Configurazione corretta di firewall aziendali.
- Monitoraggio del traffico di rete per comportamenti sospetti.

CYBER SECURITY IN AZIENDA

30 STRATEGIE

06

Crittografia Dati

- Crittografia dei dati a riposo e in transito.
- Implementazione di protocolli crittografici avanzati (es. AES-256).

07

Backup e Ripristino

- Backup automatici e regolari dei dati critici.
- Test dei processi di ripristino dei dati per garantire l'integrità.

08

Segmentazione della Rete

- Separazione delle reti pubbliche e private.
- Limitazione dell'accesso a determinate parti della rete in base al ruolo.

09

Protezione degli Endpoint

- Implementazione di soluzioni di sicurezza per endpoint.
- Monitoraggio continuo e protezione dai malware.

10

Politiche di Accesso e Permessi

- Accesso basato sul principio del "minimo privilegio".
- Revisione regolare dei permessi di accesso.

CYBER SECURITY IN AZIENDA

30 STRATEGIE

11

Monitoraggio dei Log

- Monitoraggio continuo dei log di sicurezza e di sistema.
- Implementazione di sistemi di log centralizzati per il rilevamento di minacce.

12

Protezione dei Dispositivi Mobili

- Implementazione di politiche di sicurezza per i dispositivi mobili (MDM).
- Crittografia dei dispositivi mobili aziendali.

13

Prevenzione delle Perdite di Dati (DLP)

- Implementazione di soluzioni DLP per prevenire la perdita o il furto di dati.
- Monitoraggio delle e-mail e delle comunicazioni aziendali.

14

Formazione del Personale

- Formazione continua dei dipendenti sulla sicurezza informatica.
- Simulazioni periodiche di phishing per valutare la consapevolezza.

15

Politiche di Sicurezza Remote Work

- Implementazione di VPN sicure per i dipendenti in smart working.
- Controllo dell'accesso remoto con autenticazione MFA.

CYBER SECURITY IN AZIENDA

30 STRATEGIE

16

Protezione della Posta Elettronica

- Filtri antispam e antivirus per le e-mail.
- Implementazione di protocolli come SPF, DKIM, DMARC per autenticare le email.

17

Protezione da Attacchi Phishing

- Formazione e sensibilizzazione sui pericoli del phishing.
- Strumenti automatici di rilevamento delle email di phishing.

18

Politiche di Sicurezza Cloud

- Verifica dell'implementazione di misure di sicurezza sui servizi cloud.
- Crittografia dei dati memorizzati nel cloud.

19

Controllo degli Accessi Fisici

- Limitazione dell'accesso fisico ai server e alle aree critiche.
- Implementazione di badge e dispositivi biometrici.

20

Test di Penetrazione

- Esecuzione regolare di test di penetrazione per identificare vulnerabilità.
- Implementazione di piani di mitigazione basati sui risultati dei test.

CYBER SECURITY IN AZIENDA

30 STRATEGIE

21

Piano di Risposta agli Incidenti

- Definizione di un piano chiaro di risposta agli incidenti di sicurezza.
- Formazione del personale chiave per rispondere a violazioni di sicurezza.

22

Protezione contro gli Attacchi DDoS

- Utilizzo di servizi di mitigazione DDoS per proteggere le risorse online.
- Monitoraggio del traffico di rete per rilevare attacchi in corso.

23

Policy di BYOD (Bring Your Own Device)

- Definizione di regole per i dispositivi personali che accedono alla rete aziendale.
- Implementazione di misure di sicurezza per il BYOD, come MDM.

24

Protezione delle API

- Implementazione di controlli di sicurezza per le API esposte.
- Utilizzo di protocolli sicuri per l'autenticazione e la comunicazione delle API.

25

Sicurezza dei Database

- Crittografia dei database critici.
- Controllo degli accessi e monitoraggio delle attività sui database.

CYBER SECURITY IN AZIENDA

30 STRATEGIE

26

Monitoraggio delle Minacce

- Implementazione di un Security Information and Event Management (SIEM) system.
- Monitoraggio in tempo reale delle potenziali minacce.

27

Analisi del Rischio

- Valutazione regolare dei rischi associati ai sistemi informativi.
- Identificazione e mitigazione delle vulnerabilità.

28

Normative e Compliance

- Rispetto delle normative di sicurezza (GDPR, ISO 27001, PCI DSS, ecc.).
- Verifica continua della conformità alle leggi e regolamenti vigenti.

29

Accesso ai Fornitori e Terze Parti

- Limitazione dell'accesso di fornitori esterni ai sistemi interni.
- Implementazione di controlli di sicurezza per fornitori e partner terzi.

30

Vulnerability Management

- Scansione regolare delle vulnerabilità e applicazione delle patch.
- Implementazione di processi di gestione delle vulnerabilità.

LI CONOSCEVI GIA' TUTTI ?

RICHIEDI QUI UN AUDIT GRATUITA DEI TUOI SISTEMI IT

tnsolutions.it
FINE TECHNOLOGY