Via Crispi 19 – 21100 Varese –
tel: 0332 804723 e-mail: info@ghirosrl.it - Pec ghiro.srl@legalmail.it
C.F., p.IVA e registro imprese: 03274410129 - - Cap.soc. 30.000€ i.v.

CIRCOLARE PRIVACY – GENNAIO 2025

➔ Autenticazione a più fattori per proteggere computer

Le nuove Linee Guida dell'Agenzia per la Cybersicurezza Nazionale (ACN) del novembre 2024 introducono l'obbligo di autenticazione a più fattori per proteggere computer, dispositivi e banche dati. Questa misura, raccomandata in risposta a recenti episodi di accessi abusivi a banche dati di rilevanza nazionale, mira a rafforzare la sicurezza informatica, superando la sola protezione tramite password.

Punti principali:

1. **Autenticazione a più fattori**: l'accesso ai sistemi richiede l'uso combinato di una password e di un secondo elemento, come codici temporanei inviati via sms. Viene raccomandata la generazione di password casuali complesse e la disinstallazione di software non necessari.
2. **Misure di sicurezza:** le linee guida comprendono controlli tecnici, fisici, giuridici e organizzativi. Tra queste:
    1. Sistemi di allarme contro accessi non autorizzati.
    2. Test di penetrazione periodici.
    3. Controllo dell'accesso fisico ai locali.
    4. Clausole di cybersicurezza nei contratti.
    5. Formazione obbligatoria per il personale, soprattutto quello con accessi privilegiati.
3. **Obiettivi**: non solo la protezione dei dati personali (come previsto dal GDPR), ma anche la garanzia della continuità operativa.
4. **Monitoraggio e auditing:** sistemi centralizzati per il log degli eventi e la revoca tempestiva delle credenziali ai fornitori alla fine delle collaborazioni.

Queste indicazioni anticipano ulteriori obblighi normativi che saranno definiti ad aprile 2025, nell'ambito della normativa NIS 2 (d.lgs. 138/2024). *Fonte: Italia Oggi - di Antonio Ciccia Messina*

Autovalutazione

- Sono definiti e documentati i livelli di privilegi di accesso per ciascun utente in base al ruolo aziendale?
- Esistono procedure per monitorare e revocare tempestivamente le credenziali di accesso di dipendenti o fornitori cessati?
- Sono installati sistemi di rilevamento automatico degli accessi non autorizzati o sospetti?
- Abbiamo adottato firewall, sistemi di log centralizzati e strumenti di auditing per monitorare eventi e potenziali minacce?
- Sono stati implementati programmi di sensibilizzazione per tutto il personale sui rischi e sulle buone prassi di sicurezza informatica?
- Svolgiamo regolarmente test di penetrazione per identificare vulnerabilità nei nostri sistemi?
- I dispositivi obsoleti sono smaltiti in modo sicuro per prevenire perdite di dati?
- Il personale con accessi privilegiati ha ricevuto una formazione specifica in materia di cybersicurezza?

Grazie dell'attenzione

Per ogni informazione scrivere a katia.langini@ghirosrl.it