STUDIO ASSOCIATO
LORENZO E RICCARDO PERINETTO
DOTTORI COMMERCIALISTI E CONSULENTI DEL LAVORO
Corso G. Matteotti, 44 – 10121 –Torino (TO) – ITALIA Tel. 0115155411 – Fax 0115624225
segreteria@studioperinetto.it - www.studioperinetto.it

Torino, 18 novembre 2025

Comunicazione n. 19

Oggetto: Sicurezza informatica, protezione dei dati personali e adempimenti GDPR

Gentile Cliente,

negli ultimi anni si è registrato un significativo aumento degli attacchi informatici rivolti alle infrastrutture aziendali, con particolare impatto sulla sicurezza dei dati personali trattati dalle imprese. Il Regolamento Europeo 2016/679 (meglio noto come GDPR) richiede che i titolari adottino **misure tecniche e organizzative adeguate** per garantire:

- **riservatezza**
- **integrità**
- **disponibilità**
- **resilienza** dei sistemi informativi.

1. Principali tipologie di attacchi e rischi per le imprese

1.1. Malware

I malware sono software malevoli progettati per compromettere, danneggiare o ottenere accesso non autorizzato ai sistemi informatici. Possono avere finalità differenti, ma rappresentano una delle minacce più diffuse.

• Ransomware: cifra i dati e richiede un riscatto.

• Trojan/Backdoor: consente accesso remoto nascosto ai sistemi.

• Spyware/Keylogger: consente di carpire informazioni e credenziali.

• Worm: si auto-propaga all'interno della rete, diffondendo l'infezione.

Rischi principali: indisponibilità dei sistemi, esfiltrazione o perdita dei dati, furto di credenziali, blocchi operativi, interruzione dei servizi, danni economici e reputazionali.

1.2. Credential stuffing e attacchi alle credenziali

Utilizzo di credenziali rubate o tentativi automatizzati per ottenere accesso a sistemi e account.

Rischi principali: accessi non autorizzati, transazioni fraudolente, compromissione di sistemi e dati.

1.3. Compromissione casella e-mail (BEC – Business Email Compromise)

Accesso illecito alle caselle email aziendali, con possibilità di intercettare, manipolare o falsificare comunicazioni.

Rischi principali: frodi finanziarie, diffusione indebita di dati, manipolazione dei rapporti con clienti e fornitori.

1.4. Attacchi DDos

Attacchi che sovraccaricano i server o i servizi per renderli indisponibili agli utenti legittimi.

Rischi principali: indisponibilità dei servizi, impossibilità di accedere ai sistemi, interruzione operativa.

1.5. Errori e rischi interni (human factor)

Il fattore umano è una delle cause più frequenti di violazioni. Esempi:

- accessi impropri o esfiltrazione da parte di dipendenti;
- invio a destinatari errati via email o posta;
- configurazioni errate di sistemi, database o cloud.

Rischi principali: violazioni privacy, divulgazione non autorizzata, malfunzionamenti, perdita dati.

1.6. Perdita o furto di dispositivi aziendali

Laptop, smartphone, USB e documenti cartacei sono comunemente soggetti a smarrimento o furto.

Rischi principali: accesso non autorizzato a dati sensibili, furto d'identità, elevato impatto sulla riservatezza soprattutto se i dispositivi non sono cifrati o se contengono grandi quantità di dati personali.

1.7. Social engineering e phishing

Tecniche che manipolano dipendenti e utenti (es. phishing, spear phishing, vishing) per rubare credenziali, installare malware, ottenere pagamenti fraudolenti.

I casi di furto d'identità e compromissione e-mail aziendali devono essere trattati come violazioni importanti da notificare al Garante Privacy.

2. Misure minime di prevenzione e sicurezza (tecniche e organizzative)

2.1. Misure tecniche

Aggiornamenti e patch management

- Mantenere aggiornati sistemi operativi, applicativi, firewall, router e dispositivi Wi-Fi
- Documentare e monitorare gli aggiornamenti

Backup sicuri e testati

- Backup separati e non accessibili dal sistema principale (metodo 3-2-1)
- Test periodici di ripristino
- Copie incrementali e complete

Segmentazione e isolamento della rete

- Reti separate per server critici, utenti, guest Wi-Fi, sistemi OT/IoT

Antimalware, firewall e sistemi di rilevamento intrusioni (IDS/IPS)

- Monitoraggio continuo
- Log inviati a un server centrale non modificabile

Cifratura dei dati

- Cifratura at-rest e in-transit per dati sensibili
- Gestione sicura delle chiavi

Autenticazione forte (MFA)

- Obbligatoria per account amministrativi, VPN, sistemi cloud
- Consigliata per tutti gli utenti

Password sicure e strumenti di gestione

- Policy robuste
- Password manager
- Limitazione tentativi di login

Test di vulnerabilità e penetration test periodici

- Almeno annuali o dopo cambiamenti infrastrutturali

2.2. <u>Misure organizzative</u>

Formazione continua del personale

Politiche interne aggiornate

Piano di risposta agli incidenti (IRP)

- Ruoli e responsabilità
- Contatti esterni (forensic, CERT, legale)
- Procedure per contenimento, analisi, ripristino

Business Continuity e Disaster Recovery

- Procedure per incidenti gravi
- Test periodici

Gestione fornitori

- Clausole contrattuali GDPR
- Penetration test e audit
- Verifica effettiva delle misure di sicurezza

3. Raccomandazioni finali

Le imprese devono considerare la sicurezza informatica come parte integrante della compliance al GDPR. Gli attacchi informatici non rappresentano solo un rischio operativo, ma possono comportare danni economici significativi, perdita di dati e fermo attività, danni reputazionali, pesanti sanzioni amministrative.

Rafforzare la postura di sicurezza, adottando le misure illustrate, consente di ridurre drasticamente la probabilità e l'impatto degli incidenti.

*****

Se desidera valutare il livello di adeguatezza della Sua organizzazione — sia sotto il profilo documentale che informatico — rispetto al GDPR, o se non ha ancora provveduto ad adottare le misure richieste dalla normativa europea in materia di protezione dei dati personali, può rivolgersi all'ufficio legale interno, contattando lo Studio ai consueti recapiti.

Cordiali saluti.

STUDIO ASSOCIATO

LORENZO E RICCARDO PERINETTO