Ordine dei Dottori Commercialisti e degli Esperti Contabili di Torino

ORDINE DEGLI AVVOCATI DI TORINO

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI TORINO

Tavolo di lavoro congiunto "Protezione dei dati personali – GDPR

OdV e Privacy: aggiornamenti ai tempi del COVID

Riflessioni sul tema

a cura del Referente del TdL congiunto «Protezione dei dati personali – GDPR»
Ordine Ingegneri della Provincia di Torino

Paolo Traversa *Ingegnere*

TaxLawPlanet™ *Webinar*

Torino, 22 giugno 2020

231

Osservanza

Efficacia

Attuazione

Aggiornamento

Aspetti rilevanti di rischio

Valutazione mod 231 e adeguamento

- SmartWorking
- Protocollo COVID-19
- Sicurezza del lavoro:

Aspetti rilevanti di rischio dello smart working- aspetti tecnici

- Situazioni reali che possono portare rischi:
  - Uso di strumenti non aziendali (pc personali e condivisi, antivirus/ antimalware non presenti o non aggiornati)
  - *Shadow it* uso di strumenti cloud non aziendali (WeTransfer, Dropbox personali, Drive personali…)
  - Abitudine all'utilizzo di strumenti in modalità remota
  - Disponibilità di risorse centrali per un numero di utenti MOLTO superiore al normale
- E ricordiamo che …

Rischi

Phishing	• Mail/ messaggi che invitano a inserire utenze e password su siti che *assomigliano* agli originali ma servono solo per rubare le credenziali
Malware	• Software che (magari all'interno di altri) si propaga nella rete aziendale e danneggia dati e ambiente
Ransonware	• Tipologia di malware che cifra i dati e chiede un pagamento per sbloccarli

Rischi

Social engineering	• Recuperare informazioni spacciandosi per colleghi/ responsabili aziendali
Shadow IT	• Uso di strumenti di condivisione (tipicamente cloud) non aziendali es Wetransfer/ Gdrive-OneDrive *gratis*
Uso non corretto di strumenti aziendali	• Se il repository dati è pensato per essere usato da server non bisogna copiarlo in locale (potrebbe intaccare l'integrità del dato)

Best practices

Backup

Salvataggio giornaliero su dispositivi esterni/ cloud

Password

Usa password robuste (>8 caratteri con numeri/ simboli/ maiuscole-minuscole)

Cambiale spesso (almeno una volta al mese)

Antivirus

Installa e mantieni aggiornato un antivirus

Best practices

Social engineering

Attenzione a tentativi di accesso mediante relazioni di fiducia, non condividere informazioni con terzi non autorizzati

VPN

Usa connessioni sicure (e cifrate) verso la tua azienda

Condivisione

Non usare strumenti «gratuiti» per la condivisione: se non paghi qualcosa il pagamento potrebbero essere i tuoi dati

Best practices

Crittografia

Utilizza strumenti per la cifratura (rendere i dati non leggibili da non autorizzati) per mail e dati sensibili

Procedure

Implementa o segui le procedure di sicurezza aziendali (quali software utilizzare, quali azioni fare, come gestire data breach/ perdite dati)

Accessi

Tracciare accessi (login/ logout) ai sistemi ed ai posti di lavoro

Aspetti rilevanti di rischio – sicurezza sul lavoro

- Sicurezza del lavoro:
  - Responsabilità su prevenzione – Protocollo COVID-19
    - Accessi
    - Spazi comuni
    - DPI
    - Sanificazione
    - In caso di infezione
  - Responsabilità per condizioni di smart working
    - Ambienti *casalinghi* (rischio non controllato)
    - Infezione a casa??!?

Aspetti rilevanti di rischio – illeciti amministrativi

- Reati societari
- False comunicazioni societarie/ bancarotta
- Usura