Note tecniche affrontate durante il seminario GDPR

- Software per memorizzazione e gestione password: **Keepass** (https://keepass.info/)
- Servizi di generazione password sicure: https://passwordsgenerator.net/ o lo stesso Keepass
- Policy minima per l'utilizzo di password sicure:
  - lungezza di almeno 10 caratteri
  - almeno una lettera maiuscola
  - almeno una lettera minuscola
  - almeno un numero
  - almeno un carattere speciale (es. #, @, !, $, %, …)
- Esempi di password da evitare: date di nascita, nomi di figli o coniugi, nomi di animali domestici, nomi di squadre del cuore, ecc
- Esempio di password sicura: %MyS3cur$P4ssw0rd!
- Misure tecniche basilari da adottare per proteggere adeguatamente il sistema ed i dati in esso contenuti:
  - Autenticazione all'avvio del sistema
  - Assegnazione di account diversi per ogni utilizzatore della postazione di lavoro
  - Ove possibile, utilizzo di utenze non amministrative
  - Scegliere password diverse per ogni singolo servizio; non utilizzare, dunque, la stessa password per la posta elettronica, per i social networks (es. LinkedIn o Facebook), per servizi bancari online, ecc.
  - Restrizione di permessi per file in condivisione (es. cartelle condivise o servizi in cloud)
  - Eseguire periodicamente il backup dei propri dati su supporti esterni
  - Eseguire periodicamente aggiornamenti del Sistema Operativo
  - Evitare assolutamente di installare programmi non licenziati
  - Cifrare l'intero disco (preferibile) ed eventuali supporti esterni, o quantomeno la porzione nella quale vengono salvati i dati personali. Software: Bitlocker incluso in Windows 7/8/10, FileVault incluso in Mac OS, Luks incluso in Linux

- Installare ed aggiornare periodicamente l’antivirus (es. Avira, Kaspersky, AVG)
- Installare ed aggiornare periodicamente software anti-spyware e/o anti-malware (es. SpyBot Search & Destroy, Malwarebytes)
- Utilizzare sistemi di virtualizzazione per aprire e consultare in maniera preventiva file di cui non si è certi della loro lecità. Software: VMware Player, Virtualbox.
- Abilitare e configurare a dovere il firewall all’interno del Sistema Operativo
- Cancellare periodicamente vecchie mail di cui non è più necessaria la conservazione
- In casi più strutturati e complessi (es. aziende con centinaia di dipendenti) impiegare soluzioni professionali di sicurezza informatica: sonde IDS/IPS per il “detection” ed il “prevention” di eventuali intrusioni informatiche, appliance firewall per un controllo adeguato del traffico di rete, software SIEM per il monitoraggio di incidenti informatici (es. IBM QRadar, MicroFocus ArcSight, Splunk), autenticazione centralizzata per la gestione degli accessi all’interno dell’azienda (es. Active Directory)

Latina, 03/07/2018

Ing. Francesco Ficarola