Unit 8: How to Evaluate and Apply Applicable Security Standards

Objectives:

- Review and discuss a number of GDPR related case studies.
- Review standards web sites.
- Discuss case studies and standards on the forum.

Outcomes:

- Explain which GDPR regulations are applicable to their assigned website.
- Describe which other standards their assigned website needs to meet.
- Advise on mitigations to help a website meet any of the standards applicable to its specific industry, such as data and privacy (GDPR) or financial (PCI-DSS).

Reflection:

Regulations governing the collection and use of personal data from EU citizens are provided by the General Data Protection Regulation (GDPR) (EU). Although a webpage does not explicitly promote products or services to EU residents, it must abide by the Regulation because it applies to all websites that draw European users (Yuan and Li, 2019). Companies outside of the European Union (EU) face responsibilities under this law as long as they gather or target information about EU citizens. May 25, 2018 was the date when the rule went into force. According to the new legislation, fines for breaking the GDPR's privacy standards may reach tens of millions of euros. (Pawlicka et al., 2020).

The GDPR signifies Europe's firm stance on data protection and privacy at a time when a growing number of people are turning up their private information to digital businesses. GDPR compliance may be a burden for organizations and people because of the regulation's breadth, complexity, and lack of clarity. The following are the basic tenets of GDPR: (Frankenfield, 2020)

- Lawfulness, fairness and transparency
- Storage limitation
- Purpose limitation
- Accountability
- Accuracy
- Data minimization
- Integrity and confidentiality

References

Frankenfield, J. (2020). *General Data Protection Regulation (GDPR)*. [online] Investopedia. Available at: https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp. [Accessed 22 May 2022]

Pawlicka, A., Jaroszewska-Choras, D., Choras, M. and Pawlicki, M. (2020). Guidelines for Stego/Malware Detection Tools: Achieving GDPR Compliance. *IEEE Technology and Society Magazine*, [online] 39(4), pp.60–70. doi:10.1109/MTS.2020.3031848. [Accessed 22 May 2022]

Yuan, B. and Li, J. (2019). The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation. *International Journal of Environmental Research and Public Health*, [online] 16(6), p.1070. doi:10.3390/ijerph16061070. [Accessed 22 May 2022]