TEAM NEBULA

NETWORK AND INFORMATION SECURITY MANAGEMENT

SEMINAR 4: SECURITY STANDARDS

23/06/21

Questions to answer

- **Which of the standards discussed in the sources above would apply to the website/ organisation assigned to you for the assessment?**
  We are testing an e-commerce website so the standards that would apply are:
  - GDPR
  - PCI-DSS

- **Evaluate your assigned website against the appropriate standards and decide how you would check if standards were being met?**
  Complete an assessment of the website based on the principles noted below and determine if there are controls in place to meet the standards. Determine if the controls are in place, partial or not in place and then review based on risk.
  - For **GDPR**:
    Lawfulness, fairness & transparency, Purpose Limitation, Data Minimisation, Accuracy, Storage Limitation, Integrity & Confidentiality [This could be achieved via a Pen Test], Accountability
    Ensure rights of individuals are met as per: to be informed, of access, to rectification, erasure, restrict processing, data portability, to object and automated decision making / profiling.
  - For **PCI-DSS**:
    PIN Security, Card Protection - Physical & Logical, Token Service Provider, PIN Transaction Security Point of Interaction, Payment Application Data Security Standard, PTS Hardware Security Module, Point-to-Point Encryption, 3-D Secure Software Development Kit, Software-based PIN Entry on COTS, Secure Software, Secure Software Lifecycle, Contactless Payments on COTS, 3-D Secure (3DS) Core

    For both GDPR and PCI-DSS, external audits can be conducted to identify gaps and determine how well the standards are being met.

Questions to answer

- What would your recommendations be to meet those standards?
  - Risk-based approach
    - Identify the risk appetite - how adverse to risk do they want to be, are they willing to accept the risk?
    - Outline key critical or high risks
      - Fixing the most severe issues first, till an acceptable level of risk is reached (as determined by the client)
  - Timeline of compliance goal e.g. we will be compliant in 12 months
  - Identify costs and budget available

- What assumptions have you made?
  - That the website may be subject to the scope of GDPR; however, even if this was not the case, we would adhere to other privacy standards as GDPR is only one of many. Essentially this is still good practice and should be followed.