Unit 8 Seminar 4 Preparation - Security standards

Jonathan Callaghan 19/01/2022

ICO (2020) **Guide to the General Data Protection Regulation** (GDPR).

PCI Security Standards.org (2020) Official PCI Security Standards Council Site - **PCI Security Standards Overview**.

HIPAA (2020) HIPAA For Dummies – **HIPAA Guide**.

- **Which of the standards discussed in the sources above would apply to the website/ organisation assigned to you for the assessment?**

  For example, a company providing services to anyone living in Europe or a European-based company or public body would most likely be subject to GDPR. A company handling online payments would most likely need to meet PCI-DSS standards.

Customersrus.co.uk

GDPR

General Data Protection Regulation (EU) 2016/679 (GDPR)

PCI Standards

PCI-DSS

Token Service Provider (TSS)

Point to point encryption (P2PE)

Secure software

Secure software lifecycle (Secure SLC)

PCI 3-D Secure Core (3DS)

- **Evaluate your assigned website against the appropriate standards and decide how you would check if standards were being met?**

GDPR:

1. No privacy policy was found (Article 13)
2. Outdated security controls of the site (Article 5(1)(f), Article 24(1) and Article 32. 18 software known vulnerabilities and four software outdated.
3. HTTPS encryption is missing or weak (Article 32)
4. Cookie protection – personal or tracking information are sent without a secure flag (Article 32)
5. The cookie disclaimer was not found. (Article 13)

Payments:

6. The site is outdated and needs to be patched and protected from vulnerabilities PCI DSS 6.2
7. PCI DSS 6.5 There are publicly known vulnerabilities that address secure code vulnerabilities
8. PCI DSS 6.6 installation of WAF Web Application Firewall.

- **What would your recommendations be to meet those standards?**

1. Privacy policy: Data controller needs to provide a visible notice to the data subject when personal data is collected.
2. The website needs to be secure with implementation, testing and maintenance of adequate security control to protect personal data with up-to-date web application software and regular security testing.
3. Implementation of encryption of personal data when being sent or retrieved via a browser or API. Make sure security is configured correctly.
4. Implementation of protection of personal data and encryption when they have identifiers to subjects.
5. EU Directive requires website operators to obtain informed data subject's consent before setting any cookies except strictly necessary cookies.
6. Ensure all components and software are protected from known vulnerabilities by installing vendor-supplied security patches. Install critical security patches within one month of release.
7. Address common coding vulnerabilities in software development processes by training developers annually in up to date techniques and developing applications based on secure coding guidelines.
8. Review applications and install WAF intended to reduce the compromises on pubic facing web applications due to poor coding or application management practices.

- **What assumptions have you made?**

There are apparent vulnerabilities in the website. This poses a risk to site users concerning their personal and payment data. Payments could be made to the company Sugar CRM for their service, exposing them to threat actors. The evaluation is not disastrous, as this could be rectified by following the recommendations listed above; however, the website in its current state is in a precarious position. Considering the suggestions mentioned, a more robust security policy and implementation would improve.