Haekka

Lesson 3 | Best Practices for PCI

Updated 2020-09-30

Best Practices

PCI, as a part of their guidance on PCI DSS, provides specific guidance on best practices. The basis of PCI best practice guidance states that security controls be *implemented into business-as-usual (BAU)*. This is similar to the concept of data protection by default and design from GDPR Article 25.

The best practices are broken down into 6 recommendations, which at a high level are best practices for any information security management system (ISMS).

1. **Monitoring**. Security systems that have been put in place, such as firewalls and access controls, need to be reviewed to ensure they are working as expected.
2. **Detect and Mitigate**. Failures in security systems should be detected, documented, and mitigated.
3. **Change Management**. Changes in infrastructure (hardware and virtual), software, and networks need to be evaluated for impact on security and compliance with PCI DSS.
4. **Changes in Organization Structure**. Similar to the above, but focused on changes to the organization such as acquisitions and mergers, to assess the impact on PCI DSS controls and scope.
5. **Review and Communicate with Employees**. Employees are the operational layer of security. Regular communication with employees and review of the implementation of security controls needs to be done.
6. **Reviewing Vendor Technologies**. On a periodic basis, at least annually, vendor technologies need to be assessed to ensure they continue to be supported by the vendor.

In addition, PCI recommends that organizations implement **separation of duties**. The concept ensures that there are independent checks on work. The engineers that implement encryption should not also act as the auditor to verify encryption.

Network Segmentation

Additionally, though not explicitly included in PCI best practice guidance, segmenting networks so that cardholder data (CHD) is isolated from other networks is a way to reduce the scope of a PCI assessment and the risk to cardholder data. Defining the scope is the first step of a PCI assessment. Segmenting your network limits the scope of your PCI assessments and reduces the risk to CHD.

Not all entities, based on size and PCI level, need to be validated for each of these best practices.

Though the requirements themselves go into great detail, PCI DSS at a high level is focused on following best practices for security.