Protokoll

1. Kurzzusammenfassung

In der Unterrichtseinheit vom 11.10.2020 wurde das Thema Krisen/Risikomanagement besprochen und anhand eines Beispiels wurde analysiert, wie man ein Risiko vermindern kann.

2. Inhalt

Krisensituation:

Um eine Krise zu überwinden, wird eine eigene Organisationsstruktur benötigt. Zudem gibt es in der Organisation jemanden, der die Kompetenzen besitzt eine Krise zu stabilisieren/ kontrollieren.

Verantwortlich um Risiko zu minimieren: Risiko kann nicht verhindert werden, jedoch minimiert

Beispiel Datenschutz:
Die EU DSGVO schafft für alle Mitgliedsstaaten der EU ein einheitliches Konzept.

Wenn ein Datenschutzvergehen in einer Organisation begangen wird, haftet die Geschäftsführung (persönlich).

NIS „Netz und Informationssicherheit“:

- Referenziert auf Richtlinie der EU NIS1
- Strafrahmen von DSTGVO werden übernommen
  - Bei nicht einhalten des Gesetzes→ Persönliche Haftung der Geschäftsführung

    Um ein Risiko zu minimieren, müssen Maßnahmen, Regeln und Policies überlegt werden.
    PLAN DO CHECK ACT

    Bei Datenschutz wird zwischen den Verantwortlichen und den Personen, die es durchführen (Auftragnehmer) differenziert.

    Bsp: Wir sind verantwortlich für eine Software im Medizinbereich

    Da die Software oft benötigt wird, ist es unser Ziel ein Standardprodukt zu realisieren.

- Wir sind für die Rahmenbedingungen der Entwicklung verantwortlich
- Unsere Aufgaben in diesem Bereich:
  - Personenbezogene Daten müssen verschlüsselt werden
    →Wie? Es müssen Regeln definiert werden, wie wir verschlüsseln
    →Kryptografische Vorgaben: welche Libraries, Vorgehensweise, Module, Algorithmen.
    Damit alle Entwickler im Team gleich vorgehen und nicht jeder eine eigene Vorgehensweise hat.
  - Benutzerverwaltung und Passwort: Passwörter müssen in die Datenbank gehasht werden. Jedoch reicht das alleine nicht aus, da einfach gehashte Passwörter, dennoch durch bsw. Dictionary attack, etc. entschlüsselt werden können.
    Durch Pepper and Salt kann ein Angriff, wie dictionary attack verhindert werden.
    Zudem sollten Passwörterbedingungen (Länge, Sonderzeichen, Ziffern usw.) festgelegt werden.
  - Umgebung der Entwickler müssen gleich sein
  - Mitprotokollierung (Logging): Es muss besprochen werden, welche Aktivitäten geloggt werden.

Active Directory:

Active Directory ist ein Verzeichnisdienst von Microsoft Windows Server. Mit dem Active Directory kann ein Netzwerk in einem Unternehmen entsprechend der realen Struktur des Unternehmens gegliedert werden. In dem Netzwerk werden dann Benutzer, Gruppen, Computer, etc. verwaltet

Meistens gibt es bei Webapplikation Tier 3 Logik:

- Tier 3 Logik: Backend-Frontend- Datenbank (liegt auf Datenbankserver)
- Tier 4 Logik: Business Logik in einem eigenen Bereich und DB in einem eigenen Bereich

GitHub

Neben den vielen Vorteilen, welche GitHub mit sich bringt, hat der Einsatz davon auch Nachteile. Jemand der eine Software kaufen möchte, möchte auch, dass diese alle Qualitäten erfüllt. Wenn GitHub verwendet wurde, muss mehr in die Sicherheit investiert werden.

Datenbanken:

Seite OWASP: Liste zu Top 10 Risiken für Webapplikation

Während den letzten Jahren war SQL Injection als ein großes und häufiges Risiko gelistet.

Lösungsvorschlag:

- Input Validierung: Wir validieren was der Benutzer reinschreibt
- Escapen: Es werden keine einfachen Anführungszeichen akzeptiert
- Stored Procedures: Es werden

Wenn wir eine Software schreiben, dann kann es sein, dass eine Schwachstelle auftritt, mit dieser man nicht gerechnet hat:

Was machen wir, wenn genau dies der Fall ist?

- Wir versuchen herauszufinden, ob wir diese Schwäche in unserem System haben→ PANETRATION- TESTING→ Problem: Momentan- Aufnahme
- Daher brauchen wir ein Managementsystem: Alle handelnden Personen müssen so gut miteinander vernetzt sein, dass sie Probleme erkennen und zu den anderen vermitteln können,→ homogenes Netz

Das Wichtigste ist der Schutz der CIA- Triade.

Quelle:

https://de.wikipedia.org/wiki/Active_Directory