SEIT Prüfung

1. Kryptographie:
2. 4 Beispielszenarien, sollte man symmetrische oder assymetrische Verschlüsselung nutzen
3. CBC Block zeichnen
4. **Warum wird bei CTR der Zähler verschlüsselt und nicht der Klartext? (weil Counter bekannter ist als der Klartext oder so)**
5. **Quantencomputer wird immer weiter entwickelt, warum nutzt man asymmetrische Verschlüsselung weiterhin? (Quantencomputer haben aktuell nicht genug Qubits oder so)**

* Es stehen zu wenig QBits zur Verfügung bei aktuellen Prototypen. Der beste Algorithmus braucht 2k+3QBits. Aktuelle Prototypen sind nicht fehlerfrei und für die Fehler Korrektur werden mehr Bits benötigt

1. :
2. Sie haben ein Unternehmen in Security Testing, welche drei konkreten Maßnahmen brauchen Sie um von Reifegrad 2 auf Reifegrad 3 in SSE-CMM zu kommen?
3. Sie haben ein Softwareunternehmen für Sicherheit in Supply Chains, warum ist OpenSAMM nicht geeignet hierfür?
4. OWASP Testing Framework auf MSDLC abbilden (auf die verschiedenen Stufen)
5. Risikoanalyse unter Verwendung von OWASP Risk Rating für eine Online Banking Webseite durch. (Passwort von Kreditkare rausfinden, Threat Agent und Vulnerability). Sie betrachten „Durchprobieren von Passwörtern beim kundenlogin“. Welchen Angreifer nehmen Sie an? **Cyber Krimineller**.

* Geben Sie für diese Bedrohung die Bewertungen für die Faktoren „Threat Agent“ und „Vulnerability“

**Skill Level:9**

**Motive:9**

**Opportunity:9**

**Size:9**

* Welche Wahrscheinlichkeit hat diese Bedrohung ?

**Ease of Discovery:9**

**Ease of Exploit:9**

**Awarness:9**

**Intrusion Detection:**

1. Security Pattern für VPN Zugang:
2. Welche Akteure sollte es geben? **Benutzer, Security Operations**
3. Welche Komponenten sind essenziell?
4. 8 Security Controls aus dem Katalog und auf welche Komponenten sind sie übertragbar
5. Pattern zeichnen
6. :
7. **Klimaaktivisten sprühen Boden mit Kühlspray um Ampeln auf Rot zu schalten, Angreifer in Hof-Piskow Modell zeichnen**
8. Misuse Case Diagramm (Professor, Prüfungsamt, Noten speichern)
9. **Wie werden Angreifermodelle in UMLsec dargestellt und wie können sie zur Verbesserung von Sicherheitsaspekten genutzt werden?**