1277EMWi01 Ergänzungsmodul Wirtschaftsinformatik I
71105 Informationssicherheit und IT-Forensik

15.02.2019

Prüfer: ***Dipl. Wirt.-Inf. Martin Wundram***

ÜBUNGSKLAUSUR ohne Wertung

Umfang der Klausuraufgabe: 3 Seiten

Bearbeitungsdauer: 90 Minuten (Übungsdauer 90 Minuten)

In dieser Übungsklausur sind maximal 90 Punkte zu erreichen. ~~Sie ist in der Regel bestanden, wenn mindestens 45 Punkte erreicht wurden.~~ Es sind alle Aufgaben zu bearbeiten – es gibt keine Auswahlmöglichkeiten.

Die Klausur besteht aus drei Teilen A, B und C mit jeweils maximal 30 erreichbaren Punkten. Bitte achten Sie bei der Beantwortung der Aufgabenteile auf eine stringente Gliederung Ihrer Antwort, da die Gliederung mit in die Bewertung einfließt. Falls Ihnen ein Fachbegriff oder eine Definition nicht exakt einfällt, können Sie durch schlüssige und präzise Umschreibung dennoch Teilpunkte erreichen. Achten Sie außerdem auf die Lesbarkeit Ihrer Schrift, da schlecht lesbare Lösungsvorschläge mit Null Punkten bewertet werden.

Bitte tragen Sie alle Ihre Antworten in die ausgegebenen Lösungshefte ein. Ausführungen oder Ankreuzungen auf den Aufgabenblättern werden nicht gewertet.

Bitte tragen Sie Initialen und Ihre auf dem Mantelbogen aufgedruckte Matrikelnummer oder Prüfungsnummer auf dem Lösungsheft ein.

Das Lösungsheft ist nach Bearbeitung der Aufgaben in den ausgelegten Mantelbogen einzulegen.

Viel Erfolg!

Teil A – Allgemeine Aspekte und IT-Forensik *(30 Punkte)*

Aufgabe 1 – Definition und Grundüberlegung „Sicherheit“
Definieren Sie die Begriffe „Safety“ und „Security“ und grenzen Sie diese voneinander ab. Definieren Sie dann den Begriff Sicherheit. Erklären und begründen Sie, ob es in einem offenen und interagierenden System 100% Sicherheit geben kann, oder nicht.

(8 Punkte)

Aufgabe 2 – Definition und Grundüberlegung Sicherheitslevel
Erläutern Sie, was unter dem Begriff „optimales Sicherheitslevel“ zu verstehen ist. Ist dieses für alle Unternehmen gleich? Warum / warum nicht?

(5 Punkte)

Aufgabe 3 – Definition „Fehlertolerantes Computersystem“
Definieren Sie, was ein fehlertolerantes Computersystem ist.

(2 Punkte)

Aufgabe 4 – Web-Security
Wofür steht die Abkürzung „XSS“? Was ist eine XSS-Schwachstelle? Skizzieren Sie mögliche Gegenmaßnahmen.

(5 Punkte)

Aufgabe 5 – DSGVO
Wofür steht die Abkürzung „DSGVO“? Nennen Sie drei der sieben Grundsätze nach Art. 5 der EU-DSGVO.

(4 Punkte)

Aufgabe 6 – IT-Forensik
Was besagt die Locard‘sche Regel? Geben Sie ein Beispiel aus dem Bereich der IT.

(2 Punkte)

Aufgabe 7 – IT-Forensik 2
Was ist „Carving“ und warum liefert diese Technik auf nahezu jedem Datenträger sinnvolle Ergebnisse? In welchen Situationen wird man mitels „Carving“ keine sinnvollen Ergebnisse erzielen können?

(4 Punkte)

Teil B – Kryptographie *(30 Punkte)*

Aufgabe 1 – Definition Einwegfunktion
Was bedeutet es, wenn eine Funktion eine Einwegfunktion ist? Nennen Sie ein Beispiel für eine kryptographische Einwegfunktion.

(4 Punkte)

Aufgabe 2 – Modulo-Berechnungen
Berechnen Sie geschickt, d.h. unter Angabe von Zwischenschritten:

1. $2^{23} \bmod 31$
2. $2^{11} \bmod 17$

3. 6^5 mod 30
4. 4^{128} mod 5

(8 Punkte)

Aufgabe 3 – RSA-Algorithmus
Für den RSA-Algorithmus seien folgende Parameter vorgegeben: p=5, q=7, e=7
Berechnen Sie den öffenlichten und privaten Schlüssel zu diesen Parametern. Zeigen Sie auch, wie Alice die Nachricht M=3 an Bob verschlüsseln kann, und wie dieser Sie mit seinem privaten Schlüssel wieder entschlüsselt.

(10 Punkte)

Aufgabe 4 – Diffie-Hellman-Schlüsselaustausch
Alice und Bob wählen für den Diffie-Hellman-Schlüsselaustausch die gemeinsamen Parameter n=29 und g=2. Weiterhin wählt Alice den geheimen Parameter 5, Bob den Parameter 11. Berechnen Sie jeweils für Alice und Bob den durch den Diffie-Hellman-Algorithmus ausgetauschten Schlüssel.

(8 Punkte)

Teil C – Security Engineering *(30 Punkte)*

Aufgabe 1 – Definition Security Engineering
Definieren Sie den Begriff „Security Engineering". Kommt Security Engineering nur bei der Neuentwicklung von Systemen zum Einsatz oder auch bei der Weiterentwicklung? Warum / warum nicht? Nennen Sie die vier Bereiche des Frameworks von Ross Anderson.

(5 Punkte)

Sie sind Wirtschaftsinformatiker und haben den Auftrag erhalten, mittels Web-Techniken ein per Browser erreichbares Patientenportal für eine urologische Klinik zu entwickeln. Die Programmierung wird später jemand aus Ihrem Team übernehmen; Ihre Aufgabe ist es, das System inkl. aller wesentlicher Vorgaben und Architekturentscheidungen zu designen. Die zentrale Krankenhaus-IT stellt einmal pro Nacht aus dem zentralen Krankenhaus-System einen Export aller medizinischen Befundungen auf einem Export-System bereit. Ihr System soll diese Daten importieren und dann den Patienten zugänglich machen. Die Patienten sollen lediglich lesend auf diese Daten zugreifen können. Dazu sollen die Patienten sich selbst einen Account registrieren können, der dann später von einem Arzt freigeschaltet wird.

Aufgabe 2 – Festlegung Schutzbedarf / Schutzziele für das zu entwickelnde Patientenportal
Legen Sie für das zu entwickelnde Patientenportal für die drei grundsätzlichen Schutzziele und die vier erweiterten Schutzziele einen Schutzbedarf fest. Begründen Sie Ihre Entscheidung jeweils kurz.

(7 Punkte)

Aufgabe 3 – Durchführung des Security Engineering nach Top-Down-Vorgehen für das zu entwickelnde Patientenportal
(a) Führen Sie mittels Threat Tree eine (kurze) Bedrohungsanalyse durch. Definieren Sie eine Wurzel sowie einige Knoten und Blätter.

(b) Stellen Sie eine Security Policy auf, die aus 4 Sicherheitsvorgaben besteht (wählen Sie beispielhaft 4 Vorgaben nach Ihrem freien Ermessen aus) und formulieren Sie diese kurz (z.B. jeweils ein bis zwei Sätze) aus.

(c) Skizzieren Sie drei Security Mechanisms, die geeignet sind, Ihre Schutzziele zu erfüllen, die Security Policy umzusetzen und damit die erkannten Bedrohungen zu entschärfen. Begründen Sie Ihre Wahl der Mechanismen.

(18 Punkte)