2018	Wilhelm Büchner Hochschule Private Fernhochschule Darmstadt **Typ** **Übungsklausur**	Studienfach: **Sicherheit von Systemen und Netzwerken** Klausur: **SRN**

Prüfer: **Michael Best**	Studiengang: **Bachelor Angewandte Informatik**

Prüfungsdauer: **120 Minuten**

Erlaubte Hilfsmittel: **Zeichenmaterial, Standardtaschenrechner**

1. **Aufgabe: (20 Punkte) – SRN01**

a) Teilaufgabe (10 Punkte)
Eine verteilte Applikation soll erstellt werden. Die Komponenten sind Webserver und Loadbalancer. Alle Komponenten haben eine zugesicherte Verfügbarkeit von 98%. Berechnen Sie die Gesamtverfügbarkeit und die Gesamtverfügbarkeit, wenn alle Komponenten als Cluster aufgebaut werden.

b) Teilaufgabe (10 Punkte)
Stellen Sie die Vorteile (Nachteile) von einem inkrementellen Backup zu einem differentiellen Backup dar.

2. **Aufgabe: (20 Punkte) – SRN02**

a) Teilaufgabe (10 Punkte)
Worauf ist bei Passwörtern in Hinblick auf Sicherheit zu achten?

b) Teilaufgabe (10 Punkte)
Was ist ein CERT? Welches sind seine Aufgaben?

3. **Aufgabe: (20 Punkte) – SRN03**

a) Teilaufgabe (10 Punkte)
Beschreiben Sie, was mehrstufige Firewalls sind anhand eines selbst gewählten Beispiels!

b) Teilaufgabe (10 Punkte)
Was genau sind zustandsorientierte Firewalls?

4. **Aufgabe (20 Punkte) – SRN04**

a) Teilaufgabe (10 Punkte)
Was ist in der Vorbereitungsphase der IT-Forensik zu beachten?

b) Teilaufgabe (10 Punkte)
Erklären Sie den Unterschied zwischen Penetration Testing und Vulnerablity Scanning

5. **Aufgabe (20 Punkte)**

a) Teilaufgabe (10 Punkte)
Erklären Sie Perfect Forward Secrecy (PFS) anhand eines Beispiels.

b) Teilaufgabe (10 Punkte)
Welche Sicherheitstechniken sind beim Websurfen relevant?

6. **Aufgabe (20 Punkte)**

a) Teilaufgabe (10 Punkte)
Welchen Schutz gibt es beim MAC-Address Spoofing beim WLAN?

b) Teilaufgabe (10 Punkte)
Sie sind Sicherheitsbeauftragter eines Unternehmens, das BYOD einführen möchte. Was gilt es zu beachten?

2018	Wilhelm Büchner Hochschule Private Fernhochschule Darmstadt **Typ** **Übungsklausur**	Studienfach: **Sicherheit von Systemen und Netzwerken** Klausur: **SRN**

Prüfer: **Michael Best**	Studiengang: **Bachelor Angewandte Informatik**

Musterlösungen

1. Aufgabe: (20 Punkte) – SRN01

a) Teilaufgabe (10 Punkte)

Eine verteilte Applikation soll erstellt werden. Die Komponenten sind Webserver und Loadbalancer. Alle Komponenten haben eine zugesicherte Verfügbarkeit von 98%.

Berechnen Sie die Gesamtverfügbarkeit und die Gesamtverfügbarkeit, wenn alle Komponenten als Cluster aufgebaut werden.

b) Teilaufgabe (10 Punkte)

Stellen Sie die Vorteile (Nachteile) von einem inkrementellen Backup zu einem differentiellen Backup dar.

Siehe Heft SRN01:

Die Gesamtverfügbarkeit von Loadbalancer (LB) und Webserver (WS) ist: 0,98 * 0,98 = 0,96

Als Cluster hat jede Komponente eine Verfügbarkeit von (Ausfall pro Komponente: 1-0,98 = 0,02) 1 – 0,02 * 0,02 = 0,9996.

Da LB und WS in Reihe geschaltet sind, ergibt sich eine Verfügbarkeit von 0,9992 ($=0{,}9996^2$).

Inkrementelles Backup:

Beim inkrementellen Backup wird regelmäßig (idR 1x pro Woche ein Full Backup durchgeführt und dann regelmäßig (Stunde, Tag) ein Backup der Daten gemacht, die sich in diesem Zeitraum geändert haben. Das Resultat ist, dass für das Backup wenig Speicherplatz benötigt wird, im Vergleich zu einem täglichen Backup. Ebenso dauert das Zurückspielen länger, da alle Inkremente nacheinander eingespielt werden müssen.

Differentielles Backup:

Beim differentiellen Backup werden alle Daten gesichert, die sich seit dem letzten Full Backup geändert haben. Das verbraucht weniger Platz. Dafür ist es sicherer, falls eine Tagessicherung nicht erfolgreich war, aber der darauffolgende Tag erfolgreich, hat man keinen Datenverlust.

Weiter auf der nächsten Seite…

2. Aufgabe: (20 Punkte) – SRN02

a) Teilaufgabe (10 Punkte)

Worauf ist bei Passwörtern in Hinblick auf Sicherheit zu achten?

b) Teilaufgabe (10 Punkte)

Was ist ein CERT? Welches sind seine Aufgaben?

SRN02

Kap.2.2.6:

Das Betriebssystem darf nur Passwörter zulassen, die gewissen Komplexitätsanforderungen genügen (Anzahl Sonderzeichen, Ziffern, Groß-/Kleinbuchstaben), Passwörter aus der Historie verweigern und eine Mindestlänge vorschreiben. Des weiteren muss der Zugang nach einer bestimmten Anzahl von falschen EInlogversuchen gesperrt werden. (als Beispiel)

Siehe Kap. 5.1

Das CERT ist ein Team/ eine Abteilung, die präventiv und reaktiv arbeiten. Oftmals haben Firmen auch nur ein reaktives Team, welches zu einem Incident als Projektteam zusammengestellt wird.

3. Aufgabe: (20 Punkte) – SRN03

a) Teilaufgabe (10 Punkte)

Beschreiben Sie, was mehrstufige Firewalls sind anhand eines selbst gewählten Beispiels!

b) Teilaufgabe (10 Punkte)

Was genau sind zustandsorientierte Firewalls?

SRN03, Kap. 6.3 (Anwendung der Theorie) und S. 50. Hierbei ist wichtig, den TCP-Handshake zu verstehen. Die Firewall erkennt den Zustand der Verbindung und lässt nur bestimmte Pakete durch.

Siehe Kap. 5.3. Wichtig ist der Unterschied zwischen UDP (zustandslos) und TCP (zustandsbehaftet). Deshalb kann bei UDP nur der Verbindungsaufbau geprüft werden.

Weiter auf der nächsten Seite…

4. Aufgabe (20 Punkte) – SRN04

a) Teilaufgabe (10 Punkte)

Was ist in der Vorbereitungsphase der IT-Forensik zu beachten?

b) Teilaufgabe (10 Punkte)

Erklären Sie den Unterschied zwischen Penetration Testing und Vulnerablity Scanning

SRN04, Kap. 4

Sofern Zeit, was nicht immer der Fall ist, wird die Aktion vorbereitet. In der Regel wird das System ein- oder ausgeschaltet beschlagnahmt, ein Image von allen Speichern (Flüchtig und Nicht-flüchtige Speicher) gezogen. Wichtig ist hierbei, dass nachgewiesen ist, dass der Forensiker oder andere nicht die Möglichkeit hatten, die Daten zu ändern, da sonst die Beweiskette gebrochen ist.

SRN04, Kap. 2,3:

Beim Vulnerability Scanning werden potentielle Schwachstellen ermittelt, in dem die vorhandene Systemkonfiguration (Welche Anwendungen konfiguriert sind) mit einer Schwachstellen-Datenbank abgeglichen werden. Es ist hierbei nicht nachgewiesen, ob die Schwachstelle wirklich ausnutzbar ist.

Beim Penetration Test werden die gefundenen Schwachstellen getestet, d.h. es wird überprüft, ob die Schwachstelle wirklich eine solche ist.

Weiter auf der nächsten Seite…

5. Aufgabe (20 Punkte)

a) Teilaufgabe (10 Punkte)

Erklären Sie Perfect Forward Secrecy (PFS) anhand eines Beispiels.

b) Teilaufgabe (10 Punkte)

Welche Sicherheitstechniken sind beim Websurfen relevant?

SRN05, Kap.2, Kap. 4

PFS ist eine Eigenschaft von Schlüsselaustauschverfahren.

Bei TLS wird ohne PFS ein Langzeitschlüssel für die Verschlüsselung verwendet. Wird dieser aufgedeckt, kann rückwirkend der ganze Datenverkehr entschlüsselt werden. Bei PFS werden diese Langzeitschlüssel nicht dazu benutzt, Daten zu verschlüsseln, sondern nur zu Signaturzwecken. Für die Vertraulichkeit werden Sessionkeys verwendet. Wie der Name sagt, werden diese nur für eine Session verwendet. Beim Aufdecken des Sessionkeys kann somit nur die aktuelle Session entschlüsselt werden.

Sicherheitsprotokolle beim Surfen:

HTTP → Verschlüsselung mit TLS

DNS → Absicherung mit DNSSec

Server-Zertifikat → Absicherung der Authentitität des öffentlichen Schlüssel des Webservers

Client-Zertifikate: → Absicherung der Identität des Client-Browsers

Weiter auf der nächsten Seite…

6. Aufgabe (20 Punkte)

a) Teilaufgabe (10 Punkte)

Welchen Schutz gibt es beim MAC-Address Spoofing beim WLAN?

b) Teilaufgabe (10 Punkte)

Sie sind Sicherheitsbeauftragter eines Unternehmens, das BYOD einführen möchte. Was gilt es zu beachten?

SRN06, Kap.2.1.2

Das MAC-Address Spoofing ist beim WLAN sehr heikel, da die MAC-Adresse nicht verschlüsselt werden kann. Deshalb ist es wichtig, die Network-Access-Kontrollen nicht auf MAC-Adressen zu beschränken. Deshalb sollten hier RADIUS-Server eingesetzt werden, idealerweise sollte die Authentifizierung mit Zertifikaten geschehen.

SRN06, Kap.4.6

Es muss sichergestellt sein, dass das Gerät adäquat vor Angriffen geschützt ist, beispielsweise durch Antiviren-Schutz, gehärtetes Betriebssystem, etc. Unternehmensdaten sollten ausschließlich stark verschlüsselt auf dem Gerät gespeichert werden. Im Fall von Missbrauch oder Verlust muss das Gerät aus der Ferne gelöscht werden können.

Anm: Die Liste könnte beliebig fortgeführt werden. Wichtig ist, dass grundlegende Mechanismen (Authentifizierung, Vertraulichkeit von Daten) adressiert sind.