[root@netsec]>

IT Security

Klausur an der Hochschule Karlsruhe – University of Applied Science
Sommersemester 2022, Dienstag, 19.07.2022, 11:00 Uhr

Name:_____ Punkte:_____/100 (40 zum Bestehen) Note:____

Disclaimer:
- Zugelassene Hilfsmittel: keine ausser Stifte und Lineal
- Der Lösungsweg muss bei allen Aufgaben ersichtlich sein

Aufgabe 1: Begriffswelt

__/10 __/10 Punkte

Es reicht!
Das Filmangebot teilt sich zunehmend auf immer mehr verschiedene Streaming-Anbieter auf und zwingt die Kunden zu parallelen Abos oder kreativen Wegen des Filmkonsums.
Ihr innovatives Startup „FlatNix“ will einen Metastreamingdienst schaffen, der dieses Problem löst.
Das Projekt stellt natürlich einige Ansprüche an die IT Security!! Sie müssten sich perfekt damit auskennen und daher auch in der Lage sein, die passend zur Vorlesung korrekten Assoziationen zwischen den Begriffen in den Spalten A und B hier herzustellen:

Spalte A	Spalte B
Spam	Funktionsbeteiligt
Zuverlässigkeit	Topologische Maßnahme
Statische Redundanz	Protokollschwäche
Hierarchisches Modell	Blacklisting
Insel	Malware
Circuit Level Proxy	Prepared Statement
DoS	Zeitintervall
SQL Injection	Threat Modelling
Entwurfsphase	Composed of
Trojaner	Transportschicht

Aufgabe 2: Safety

A)__/7 B)__/6 C)__/6 D)__/3 E)__/3 F)__/4 G)__/4 __/33 Punkte

A) Damit „FlatNix“ ein Erfolg wird, bauen Sie es natürlich georedundant auf. Die ersten Standorte sind in Kiel (Verfügbarkeit 50%) und in Lyon (80%). Diese teilen sich das Content Delivery Network (Verfügbarkeit 90%) eines Providers und nutzen es für wichtige Teile der Benutzeroberfläche.
Wie groß ist die Ausfallwahrscheinlichkeit Ihres Dienstes?

B) Sie können Prag als dritten Standort (Verfügbarkeit: 70%) hinzunehmen. Wie verändert sich die Ausfallwahrscheinlichkeit Ihres Dienstes?

C) Das Risiko eines Ausfalls wird mit 3 Mio € bewertet. Wie ist nach ISO das Risiko definiert? Wie hoch sind demnach Ihre ungefähren Betriebskosten?

D) Fast alles in den Standorten ist mit symmetrischer Redundanz aufgebaut – in wenigen Fällen nutzen Sie allerdings asymmetrische Redundanz.
Wo und warum gerade dort?

E) Sie befassen sich mit Möglichkeiten, die Sicherheitsmechanismen von „FlatNix“ zertifizieren zu lassen. Welche der folgenden Möglichkeiten können hierzu sicherlich nicht herangezogen werden (bitte streichen):

- IT 32005
- ISO Common
- Facebook
- IT-Grundschutz
- Common Criteria
- ISO 27001
- IT Mundschutz

F) Die Verfügbarkeit von Software lässt sich eindeutig verbessern durch (bitte ankreuzen):

[ ] Optimierung der Bootzeiten
[ ] Herunterfahren der Server
[ ] Nutzung sicherer Betriebssysteme
[ ] geeignete Entwicklungsmethoden
[ ] Einsatz von Watchdogs
[ ] Vermeidung von Passwörtern
[ ] 16bit CPUs
[ ] Vermeidung von Bugfixes

G) Ihr Dienst kann grob in folgende Funktionsblöcke unterteilt werden:

- Streaming Service
- Filmedatenbank mit Suchfunktion
- Shopsystem mit Bezahlfunktion
- Benutzerverwaltung
- Homepage

Welche Schutzziele würden Sie bei den einzelnen Funktionsblöcken jeweils als sinnvoll ansehen?

Aufgabe 3: Security

A)__/6 B)__/5 C)__/4 D)__/9 E)__/4 F)__/5 G)__/6 H)__/5 I)__/6 J)__/7 __/57 Punkte

A) Vervollständigen Sie den folgenden Satz sinnvoll, da er Ihre Sicherheitsstrategie den Mitarbeitern bei „FlatNix“ gegenüber erklären hilft: „In den letzten 20 Jahren hat es bei Cyberattacken eine deutliche Tendenz zu _____ motivierten Angriffen gegeben.“
Nennen Sie mindestens zwei Beispiele an denen man das erkennen kann.

B) Welche 5 Regeln sind in Ihrer Policy die wichtigsten für die Mitarbeiter in der Software-Entwicklung?

C) Manche Mitarbeiter verwenden Tunneling-Protokolle im georedundanten RZ-Setup. Was für Gründe fallen Ihnen ein, warum Tunneling nicht eindeutig ein Sicherheitsprinzip ist, sondern auch Risiken für „FlatNix“ birgt?

D) Routing wird bei „FlatNix“ selbst gebaut. Daher ist auch die enthaltene NAT Funktionalität in Ihrer Verantwortung. Illustrieren Sie bitte in Pseudocode die Funktionsweise Ihrer NAT-Implementierung!

E) Bei einem neu aufgebauten Dienst setzen Sie von vorne herein auf Zero Trust. Kreuzen Sie bitte an, was Sie darunter verstehen:

[ ] Implizites Vertrauen
[ ] Aufteilung in Frontend und Backend
[ ] Verschlüsselte Kommunikation
[ ] Authentisierung an Übergängen
[ ] Datenhaltung stets im Kern
[ ] Absicherung auch zwischen Services
[ ] Explizites Vertrauen
[ ] DmZ

F) Am Zugang zum RZ in Lyon haben Sie einen eingehenden Paketfilter in der folgenden abstrakten Form definiert. Was für Fehler haben Sie dabei gemacht? Versuchen Sie sich an der Korrektur der Fehler.

```
ALLOW Port 80 TO ANY
ALLOW Port 22 TO ANY
ALLOW ALL
```

G) In Zusammenarbeit mit Ihrem CDN-Anbieter haben Sie XSS in Richtung der Kunden ziemlich sicher sauber ausgeschlossen. Kennen Sie noch andere Stellen an denen Ihnen XSS gefährlich werden könnte? Falls ja, erklären Sie bitte mindestens eine davon, gerne mit einer Skizze…

H) Als Sie noch während Ihres Informatik Studiums bei Gio und Fischi die IT Security Vorlesung besucht haben, haben die auch Port Scanner und ARP Spoofing erklärt. Eigentlich alter Käse. Können Sie für Ihr wichtiges „FlatNix“ Produkt erklären, warum die Themen noch eine Rolle spielen könnten?

I) Sie möchten verhindern, dass ein neidischer Wettbewerber Ihren Dienst durch eine DDoS Attacke stört. Welche Möglichkeiten haben Sie sich davor zu schützen? Welche davon würden Sie Ihrem Chef empfehlen umzusetzen? Bitte mit Begründung.

J) Identitäten spielen bei der Sicherheit eine große Rolle. Welche Identitäten auf welchen (Protokoll-) Ebenen kennen Sie bei einem öffentlichen Web-Server? Nennen Sie jeweils eine Möglichkeit, diese zu spoofen und beschreiben Sie im Sinne eines Threat Models welche Maßnahmen Sie empfehlen würden um diese Angriffe jeweils zu verhindern.