Absichern eines Mailsystems (provisorisch)

Aufgabe Block 6-12

25HS

Inhaltsverzeichnis

1 Aufgabenstellung

In den Blöcken 6-12 bauen sie eine Mailinfrastruktur mit folgenden Sicherungsmassnahmen:

- Virenscanner
- Greylisting
- SPF/DKIM
- Tarpit
- Anti-UBE
- DNSSEC

Dokumentieren sie den Aufbau dieser Infrastruktur und wie im vorliegenden Fall das Produkt abgesichert wurde. Versuchen sie die Stärken und Schwächen der von Ihnen ein gesetzten Produkte festzuhalten und zeigen Sie auf mit welchen Massnahmen Sie dies noch verfeinern könnten.

Zeigen Sie (z.B. anhand von Screenshots, Logfile-Auszügen oder Testmails), wie sie ihre Infrastruktur geprüft haben und begründen sie, wie sie zum Schluss kommen, dass ihre Infrastruktur richtig funktioniert.

Halten sie ferner fest, wie eine solche Infrastruktur in einem Produktiven Umfeld betrieben werden sollten und welche Massnahmen notwendig sind um einen sicheren Betrieb gewährleisten zu können.

Wenn Sie ihre Arbeit schreiben, setzen sie immer voraus, dass jemand den Kenntnisstand eines CyberLAB-Anfängers hat. Dieser setzt sich zusammen aus einer Person, die in der Lage ist Systeme zu installieren und sich Wissen selbst anzueignen.

2 Empfohlener Zeitplan und Vorgehensweise

Folgender Zeitplan wird für die Realisation dringendst empfohlen. Ein Abweichen von diesem Zeitplan führt typischerweise (und aus Erfahrung) zu grossen, sinnlosen Problemen. Die Theorielektionen sind auch für diese Vorgehensweise ausgelegt.

Lektion 6: Theroieblock zu DNS und Mailprotokollen. Tipps zum diagnostizieren.

Lektion 7: Installation DNS; Einrichten von forward und reverse lookups; Installation von Mailserver.

Lektion 8: Einrichten von DNSSEC.

Lektion 9: einrichten von Greylisting und SPF (evtl. auch DMARC).

Lektion 10: Einrichten von DKIM.

Lektion 11: Einrichten von Spamassassin und Malware-Scanner

Lektion 12+13: Dokumentation und Debugging.

Die Aufgabe selber lässt sich von einem routinierten Ingenieur in Sachen Email innerhalb von 6h lösen. Sie werden aber für die erste Umsetzung alle Anlässe brauchen! Unterschätzen Sie den Aufwand nicht. Die Aufgabe setzt voraus, dass ihre Infrastruktur am Ende in einem Internet operabel ist (sprich mit allen anderen im Internet kommunizieren können).

3 Lieferobjekte

3.1 Abgabeform

Es soll ein Text-Dokument abgegeben werden (nur eines). Akzeptierte Formate sind (PDF-)LaTeX, Word, Libreoffice, Markdown und PDF-Dokumente.

Optional kann auch noch ein ZIP-File mit Konfigurationsdateien mitgeliefert werden (Auch hier nur eine Datei).

Die Files sollen wie folgt benannt sein:

```
<email>_<YY><SS>_aufgabe2.<Dateierweiterung>
<email>    = Ihre Email-Adresse
<YY>       = Jahreszahl (zweistellig)
<SS>       = Semesterbezeichnung (FS=Frühjahrssemester; HS=Herbstsemester)
```

Beispiel:

```
Max.Muster@students.fhnw.ch_24HS_aufgabe2.docx
Max.Muster@students.fhnw.ch_24HS_aufgabe2.zip
```

3.2 Umfang und Inhalt

Der Umfang in Seiten wird nicht vorgegeben.

Die Dokumentation soll so ausgelegt werden, dass sie ein Nachbau der Infrastruktur erlaubt. Es wird angenommen, dass Sie die Arbeit während des Labors fortwährend schreiben.

4 Demonstration

Bereiten sie sich darauf vor am Termin der 14. cysL-Lektion eine kurze, persönlich Demonstration dem Betreuer zu geben, in der sie die Wirksamkeit der von ihnen getroffenen Massnahmen untermauern können.

4.1 Termine

Abgabe muss spätestens zwei Arbeitstage vor Beginn der 14. Lektion im cysL erfolgen. Abgabe muss elektronisch an martin.gwerder@fhnw.ch erfolgen. Der Erhalt der Arbeit wird elektronisch bestätigt.

Wenn sie anstelle von Attachments Links auf eine Download-Infrastruktur verwenden, sind sie für eine korrekte Funktion der verlinkten Infrastruktur verantwortlich. Accounts seitens des Dozenten dürfen keine vorausgesetzt werden. Ein nicht funktionieren der eigenen Infrastruktur wird als “nicht abgegeben” gewertet.

Die Rückgabe der Arbeit mit der Bewertung erfolgt in der Lektion 15.

4.2 Allgemeine Hinweise

Für den Quellendeklaration, Einsatz von KI und Offenlegung gilt das Selbe wie bei der ersten Aufgabe.