1. LB2 - Allgemeine Informationen

Bei der Aufgabenstellung für die LB2 orientieren wir uns an *Best Practices für MS Windows-Umgebungen*. Sie besteht im Wesentlichen aus der Dokumentation aus einer bestehenden Umgebung der Konfiguration von bestehenden Softwarekomponenten. Wir versuchen damit die reine Installationszeit zu reduzieren und den Erkenntnisgewinn zu maximieren.

Wir arbeiten während der gesamten Projektzeit mit einem vorgegebenen Labor. Dieses Lab implementiert Best-Practices im Umgang mit Sicherheitskonfigurationen von MS-Windows. Dabei orientiert sich die Installation möglichst an den bereits bestehenden Bordmitteln von MS Windows, was für Ihre Praxisrelevanz gut ist.

> **Danger**
>
> Sie produzieren in dieser LB2 eine Dokumentation der Installation und dieses Dokument wird bewertet.

1.1 Ablauf LB2

Der Ablauf der LB2 besteht aus den folgenden Schritten:

1. Infrastruktur aufbauen/verstehen und dokumentieren (10%)
2. Installation und Konfiguration von WSUS (und Active Directory) (20%)
3. Beschreibung der Software Sysmon (15%)
4. Beschreibung der Software OSQuery (10%)
5. Installation Winlogbeat (15%)
6. Security Dashboards ELK (15%)
7. Fleet Osquery Testing (15%)

1.1.1 Bewertungen

Sie erhalten pro 5%-Punkte ein Bewertungskriterium - welches wiederum mit dem Wertebereich 0 - 4 bewertet wird. Dies ergibt für die gesamte Arbeit eine totale Punktezahl von 80P.

1.2 Vorgaben - LB2

Gewichtung:

33%

Richtzeit (Empfehlung):

6

Element-Beschreibung:

Der Bewertung einer Arbeit, welche die Installation und Konfiguration eines komplexeren Sicherheitssystems dokumentiert.

Hilfsmittel Virtuelle:

Server- und Clientumgebung, Antimalwaresoftware

Bewertung:

Bewertungsraster mit Punkten und linearen Umrechnung in Noten nach der Formel:
Punkte*5/Maximalpunktezahl + 1

- Sicherheitskonfiguration: 50-60 % der Gesamtpunktzahl
- Updates: 10-20 % der Gesamtpunktzahl
- Dokumentation der Testergebnisse: 20-30 % der Gesamtpunktzahl

1.3 Bemerkung (das Kleingedruckte)

> **Wichtig**
>
> Ich erlaube mir von Zeit zu Zeit die Installation von Ihnen zu überprüfen und die Funktionalität schriftlich festzuhalten - diese Feststellungen fliessen in die Bewertung ein (<- "Ich will irgendwann, irgendwie etwas Laufendes bei Ihnen sehen")