

Audit-Bericht

Audit-Bericht
der von Marcel Turobin-Ort definierten technischen Policies

Auditor:	Christy Kariyampalli
Matrikelnummer:	52010080
am	Fachhochschul-Bachelorstudiengang Informatik Informatik
Auditauftraggeber:	Bleier Thomas
Wird auditoyiert:	Marel Turobin-Ort

Wiener Neustadt, 20. Mai 2023

Inhaltsverzeichnis

1	Ziel des Audit-Berichts	3
2	Systeminterne Einstellungen	4
2.1	File Vault	4
2.2	Weitere Sicherheitsmaßnahmen	4
3	Browserkonfigurationen und sicheres Surfen	5
3.1	Einstellungen	5
4	Accountsicherheit	6
4.1	Apple ID	6
5	Firewall	7
5.1	Konfiguration	7
6	Virtuelles privates Netzwerk (VPN)	8
6.1	Konfiguration	8
7	Conclusio	9

1 Ziel des Audit-Berichts

Das Ziel dieses Audits ist es, den Erfüllungsgrad der ausgearbeiteten technischen Policies und dessen Einsetzung am Rechner des Vefassers zu bestimmen. Ebenfalls werden Anmerkungen der definierten Vorgehensweisen (Arten) hervorgehoben und in den jeweiligen Kapiteln protokolliert. Zum Schluss werden allgemeine Wünsche, Verbesserungsvorschläge etc. über die verfassten technischen policies miteingebunden.

2 Systeminterne Einstellungen

2.1 File Vault

Die Verschlüsselungsmethode der Festplatte mit *FileVault* ist eine sehr gute Praxis. Die Dateien werden intern verschlüsselt und entschlüsselt, was dazu führt, dass ein Angreifer nur eine verschlüsselte Version der Dateien zur Verfügung gestellt bekommt (Falls er die Dateien auf einem anderen Rechner rüberkopiert).

2.2 Weitere Sicherheitsmaßnahmen

Der Policy-Verfasser deutet auf erweiterte Einstellungen hin, die von Voraus sein könnten und je nachdem beliebig eingestellt werden können. Ebenfalls wird erwähnt, wie der Rechner in extremen Fällen wirklich abgeschottet werden kann, indem der *Lockdown Mode* aktiviert wird. Dies hat den großen Vorteil, dass bei einem potenziellen Eindringen ins Rechner der Benutzer sofort weiß was zu tun ist und wie er sich nur in wenigen Schritten ins sichere Modus begeben und das Gerät sicher stellen kann.

3 Browserkonfigurationen und sicheres Surfen

3.1 Einstellungen

Am PC des Anwenders wurden die Browsereinstellung so konfiguriert, dass beim Surfen böartige Seiten vermieden werden können (Nur Seiten über HTTPS), ebenfalls wurde auf die Konfiguration von Zertifizierungen verwiesen, was eine wichtige Rolle spielt beim Besuchen von seriösen Seiten.

4 Accountsicherheit

4.1 Apple ID

Am Rechner des Policy-Verfassers wurde ein Apple ID eingerichtet. Das Verwenden der Apple ID ermöglicht es die 2-Faktor-Authentifizierung einzuschalten, aber auch Formen von Schlüsseln zu generieren und vertraute Geräte zu verknüpfen (Wurde ebenfalls in den technischen Policies erwähnt). Somit hat der Benutzer die Kontrolle über wer und wo sein Account und dessen bezogene Daten zugreifen kann. Eine Apple ID sollte bei jedem Mac-Gerät eingerichtet und so wie auf dem Rechner vom Marcel Turobin-Ort bestmöglichst konfiguriert werden.

5 Firewall

5.1 Konfiguration

Auch hier erwähnt der Policy-Verfasser, was für einen Nutzen es hat die Firewall einzuschalten und so gut wie möglich zu konfigurieren, und zwar, um bestimmte Verbindungen zu unterdrücken. Beim Rechner vom Marcel ist die Firewall sehr gut beziehungsweise dementsprechend, wie die policy verfasst wurde, eingestellt.

6 Virtuelles privates Netzwerk (VPN)

6.1 Konfiguration

In der technischen Policy wird erwähnt, dass VPN's gut gegen Cyberangriffe sind und unter welcher Kategorie dieser zu finden sind in der Mac-Einstellungen (Netzwerk). Dieser ist eine sehr gute Praxis und wird an sehr vielen Rechnern eingestellt/installiert.

7 Conclusio

Die technischen Policies wurden bis ins Detail ausgearbeitet und am Rechner des Verfassers angewendet. Das Mac-Gerät vom Marcel besitzt die fundamentalsten Einstellungen zur Sicherungen eines Mac-Gerätes und ist aus meiner Sicht sehr gut geschützt. Dennoch hätten vielleicht thrid-partyÄwendungen (z.B Antivirus- und Passwortsicherungsprogramme) und weitere interne Details angesprochen werden sollen. Im Großen und Ganzen ist das Verfassen und das Einsetzen der Policies dem Marcel Turobin-Ort sehr gut gelungen.