Clients unter Windows 10

Zusammenfassung

Sicherheitsanforderungen und Installationsvorgaben von Clients unter Windows 10

Diese Anleitung richtet sich besonders an folgende Zielgruppen:

- **Studierende**
- **Zweit- und Gasthörende**
- **Lehrende**
- **Mitarbeitende**
- **Einrichtungen und Gremien (z.B. Fachschaftsräte)**
- **Arbeitsbereiche / Gruppen (z.B. Projekte)**
- **Sekretariate**
- **Gäste der Friedrich-Schiller-Universität**

- Anforderungen BSI
- Umsetzung
- Checkliste

Anforderungen BSI

1. Microsofts Cloud-Dienst OneDrive deaktivieren
2. Nach einem funktionalen Update des Betriebssystems **muss** überprüft werden, ob alle Anforderungen aus dem IT-Grundschutz und den internen Vorgaben weiterhin erfüllt werden.
3. Datenschutzoptionen, Spracherkennung, Diagnosedaten, Aktivitätsverlauf und Positionserkennung sollten deaktiviert werden.
4. Sophos als Computer-Viren-Prüfprogramm installieren
5. Online-Konten zur Anmeldung von Microsoft-Konto oder Konten anderer Anbieter von Identitätsmanagementsystemen sind nicht erlaubt.
6. Alle nicht benötigten Anwendungen und Komponenten sollten deaktiviert werden.
7. Die Datenausführungsverhinderung für alle Programme und Dienste (Opt-Out Modus) aktivieren, um zu verhindern, dass Programmcodes auf eine nicht erlaubte Weise ausgeführt werden.
8. [Enterprise Version] Virtual Secure Mode (VSM) und Credential Guard aktivieren
9. Schreibrechte für den Benutzer auf bestimmten Bereich einschränken
10. kein Schreibrecht auf Betriebssystem Ordner für Benutzer
11. Die SmartScreen-Funktion deaktivieren
12. Den Sprachassistenten Cortana deaktivieren
13. Den Windows Store deaktivieren
14. Speicherung von Kennwörtern, Zertifikaten und anderen Anmeldeinformationen zur automatischen Anmeldung auf Webseiten und IT-Systemen ist nicht erlaubt.
15. Der aktuell angemeldete Benutzer sollte dem Aufbau einer Fernwartungssitzung immer explizit zu stimmen müssen.
16. Bei Verwendung des Fernzugriffes über Remote Desktop (RDP) muss die Ressourcenumleitung und die Druckerumleitung angepasst werden
17. Alle Administrator-Konten sollten dokumentiert und in regelmäßigen Abständen eingeschätzt werden.
18. Windows Powershell: Ausführen von Skripten sperren

Umsetzung

1. Systemsteuerung System und Sicherheit Verwaltung Gruppenrichtlinienverwaltung Computerkonfiguration Administrative Vorlagen Windows-Komponenten OneDrive
2. In der Standardeinstellung erhält man Sicherheitsupdates und Funktionalupdates, die von Microsoft verteilt werden.
   Man hat zusätzlich die Möglichkeit, Funktionalupdates zeitlich zu verschieben.
   Einstellungen Updates und Sicherheit Windows Update Erweiterte Optionen [Featureupdates] zurückstellen
3. Windows 10 Einstellungen Datenschutz
4. Als Virenschutz sollte Sophos verwendet werden. Das Installationspaket erhält man vom Anschlussverantwortlichen. Alternativ kann ein Standard-Installationspaket über die Webseite der Stabsstelle Sicherheit Informationstechnischer Systeme (ST-SIS) bezogen werden.
5. Systemsteuerung Programme Programme und Features
6. Systemsteuerung System und Sicherheit System Erweiterte Systemeinstellungen Erweitert Leistung Einstellungen Datenausführungsverhinderung für alle Programme und Dienste Einschalten
7. Systemsteuerung System und Sicherheit Verwaltung Gruppenrichtlinienverwaltung Computerkonfiguration Administrative Vorlagen System Device Guard Virtualisierungsbasierte Sicherheit aktivieren
8. Rechtsklick Eigenschaften Sicherheit Bearbeiten
9. Rechtsklick Eigenschaften Sicherheit Bearbeiten
10. Systemsteuerung System und Sicherheit Verwaltung Gruppenrichtlinienverwaltung Computerkonfiguration Administrative Vorlagen Windows-Komponenten Datei-Explorer Windows Defender SmartScreen konfigurieren
11. Systemsteuerung System und Sicherheit Verwaltung Gruppenrichtlinienverwaltung Computerkonfiguration Administrative Vorlagen Windows-Komponenten Suche Cortana zulassen
12. Systemsteuerung System und Sicherheit Verwaltung Gruppenrichtlinienverwaltung Computerkonfiguration Administrative Vorlagen Windows-Komponenten Store Store-Anwendung deaktivieren

13. Chrome: anpassen und einstellen Einstellungen AutoFill Passwörter / Zahlungsmethoden / AutoFill-Einstellungen
14. Systemsteuerung System und Sicherheit Verwaltung Gruppenrichtlinienverwaltung Computerkonfiguration Administrative Vorlagen Windows-Komponenten Remotedesktopdienste Remotedesktopsitzungs-Host Geräte- und Ressourcenumleitung / Druckerumleitung

Checkliste

Betriebssystem und Rechte			
	Personal Firewall		
	Anti-Spyware-Programme (z.B. Windows-Defender)		
	eingeschränkte Benutzerrechte		
		Schreibrechte für den Benutzer auf bestimmten Bereich einschränken	
		kein Schreibrecht auf Betriebssystem Ordner für Benutzer	
	OneDrive deaktivieren		
	Telemetrie und Datenschutzeinstellungen		
		Datenschutzoptionen	
		Spracherkennung	
		Diagnosedaten	
		Aktivitätsverlauf	
		Positionserkennung	
	Die Datenausführungsverhinderung für alle Programme und Dienste (Opt-Out Modus) aktivieren.		
	[Enterprise Version] Virtual Secure Mode (VSM) und Credential Guard aktivieren		
	SmartScreen-Funktion deaktivieren		
	Sprachassistenten Cortana deaktivieren		
	Windows Powershell: ausführen von Skripten sperren		
Virenscanner			
	Sophos als Computer-Viren-Prüfprogramm		
Patches und Updates			
	Aktualisierung von Windows über Update Service		
	eingesetzte Applikationen (einschließlich ihrer Erweiterungen/ Plugins) und Treiber durch automatische Update-Services oder den regelmäßigen Besuch der Hersteller-Webseiten aktualisieren		
Login Daten			
	sicheres Passwort		
	Login Daten nicht speichern oder weitergeben		
	Online-Konten zur Anmeldung von Microsoft-Konto oder Konten anderer Anbieter von Identitätsmanagementsystemen ist nicht erlaubt		
E-Mail-Programme und Browser			
	automatische Ausführen aktiver Inhalte im Browser abschalten oder einschränken		
	grundsätzlich keine Software aus Anhängen einer E-Mail ausführen		
	E-Mails mit unerwünschtem oder zweifelhaftem Inhalt nicht beachten/löschen		
	Passwörter, Kreditkartennummern, PINs, TAN niemals übermitteln		
Software			
	ausschließlich Originalsoftware verwenden und direkt vom Hersteller bzw. von einer vertrauenswürdigen Quelle beziehen		
	Alle nicht benötigten Anwendungen und Komponenten sollten deaktiviert werden		

	Windows Store deaktivieren
Aktualität und Vorsicht	
	informiert und sensibilisiert sein
Zugriffsschutz	
	Rechner nicht unbeobachtet lassen, ausloggen, Zugriff sperren, Bildschirmschoner mit sicherem Passwort aktivieren
	Administrator Konten dokumentieren und überprüfen
Datensicherung	
	Daten regelmäßig sichern
Fernwartung	
	Fernwartungssitzung nur mit Bestätigung des Benutzers
	RDP Ressourcenumleitung und Druckerumleitung anpassen