Sicherheitsrichtlinien für Telearbeitsplätze (Windows)

Zusammenfassung

Auf dieser Seiten sind Informationen zu folgenden Themen zu finden:

Diese Anleitung richtet sich besonders an folgende Zielgruppen:

- **Lehrende**
- **Mitarbeitende**
- **Einrichtungen und Gremien (z.B. Fachschaftsräte)**
- **Arbeitsbereiche / Gruppen (z.B. Projekte)**

Checkliste

1. Identifizierungs- und Authentisierungsmechanismus			
sicherheitskritische Parameter nicht unverschlüsselt gespeichert			
Kontosperrungsrichtlinien			
		Kontensperrungsschwelle: 3 ungültige Anmeldeversuche	Windows + r gpedit.msc Computerkonfiguration Windows-Einstellungen Sicherheitseinstellungen Kontorichtlinien Kontosperrungsrichtlinien Kontensperrungsschwelle
		Kontosperrdauer: 30 Minuten	Windows + r gpedit.msc Computerkonfiguration Windows-Einstellungen Sicherheitseinstellungen Kontorichtlinien Kontosperrungsrichtlinien Kontosperrdauer
		Zurücksetzungsdauer des Kontosperrungszählers: 30 Minuten	Windows + r gpedit.msc Computerkonfiguration Windows-Einstellungen Sicherheitseinstellungen Kontorichtlinien Kontosperrungsrichtlinien Zurücksetzungsdauer des Kontosperrungszählers
Kennwortrichtlinien			
		mindestens 12 Zeichen	Windows + r gpedit.msc Computerkonfiguration Windows-Einstellungen Sicherheitseinstellungen Kontorichtlinien Kennwortrichtlinien minimale Kennwortlänge
		das Passwort darf noch nie verwendet worden sein	Windows + r gpedit.msc Computerkonfiguration Windows-Einstellungen Sicherheitseinstellungen Kontorichtlinien Kennwortrichtlinien Kennwortchronik erzwingen (24)
	Bildschirmsperre nach 10 Minuten Abwesenheit		Einstellungen (Windows + i) System Netzwerkbetrieb und Energiesparen
2. Zugriffskontrolle			
	mindestens zwei Benutzergruppen (Administrator und Telearbeiter)		lokale Benutzer und Gruppen Gruppen oder Benutzer Rechtsklick neue Gruppe / neuen Benutzer
	Rechteverteilung		Datei oder Ordner Rechtsklick Eigenschaften Sicherheit Bearbeiten
		Benutzerzugriff Zugriff auf bestimmten Bereich im Dateisystem	
		Benutzer hat kein Schreibrecht in Ordnern des Betriebssystems	
3. Protokollierung			
	Protokoll darf nicht durch Unberechtigte gelesen oder manipuliert werden können		Windows + r REGEDIT.exe Computer HKEY_LOCAL_MACHINE SYSTEM CurrentControlSet Services EventLog Neuer Wert Datentyp: REG_DWORD Name: RestrictGuestAccess Wert: 1
4. Verschlüsselungskomponente			
	alle Laufwerke sind verschlüsselt		Systemsteuerung BitLocker-Laufwerksverschlüsselung BitLocker aktivieren (Anweisungen folgen)
	Schlüssel nicht unverschlüsselt gespeichert		
5. Benutzerumgebung			

	nicht benötigte Anwendungen und Komponenten deaktiviert	Systemsteuerung Programme Programme und Features Deinstallieren
	Zugriff auf spezielle Programme für Telearbeiter eingeschränkt	lokale Sicherheitsrichtlinien Anwendungsrichtlinien AppLocker Ausführbare Regeln Rechtsklick Neue Regel erstellen verweigern Programm auswählen
	unerwünschte Hardware blockiert	Gerätemanager Rechtsklick Gerät deaktivieren
	Installation von Fremdsoftware durch Telearbeiter gesperrt	Nutzer darf keine Administrations Rechte haben
6. Virenschutz		
	Sophos als Virenschutz installiert und aktiviert	Als Virenschutz Sophos verwenden. Das Standard-Installationspaket kann über die Webseite der Stabsstelle Sicherheit Informationstechnischer Systeme (ST-SIS) heruntergeladen werden.
7. Fernwartung		
	als Fernwartungstool wird ISL Light 4 angewandt	
8. VPN Verbindung		
	Cisco AnyConnect Client wird als VPN Verbindung genutzt	Um eine VPN-Verbindung aufzubauen, steht die Software Cisco AnyConnect Client zur Verfügung.
9. Datensicherung		
	Backup-Datenträger (falls vorhanden) verschlossen gelagert	
10.Power Shell		
	Power Shell beschränken	Windows + r gpedit.msc Computerkonfiguration Administrative Vorlagen Windows-Komponenten Windows Power Shell Skriptausführung aktivieren aktivieren Ausführungsrichtlinie Lokale Skripts und remote signierte Skripts zulassen
11. Firewall		
	Firewall aktiviert	Systemsteuerung System und Sicherheit Windows Defender Firewall Windows Defender Firewall ein- oder ausschalten

Umsetzungshinweise

1. **Identifizierungs- und Authentisierungsmechanismus**
   a. Sicherheitskritische Parameter, wie Passwörter, Benutzer-Kennung, usw., dürfen nicht unverschlüsselt auf dem Rechner gespeichert werden.
      Zum Speichern von Passwörtern eignet sich eine verschlüsselte Datei auf dem Rechner.
      Als Alternative eignet sich ein Passwort-Verwaltungsprogramm, um beispielsweise mehrere Passwörter zu speichern.
   b. Zugangsverfahren muss auf eine Fehleingabe reagieren, indem der Zugang zum Telearbeitsrechner gesperrt oder die Abstände vergrößert werden.
      Windows + r gpedit.msc Computerkonfiguration Windows-Einstellungen Sicherheitseinstellungen Kontorichtlinien Kontosperrungsrichtlinien
   c. Vorgaben für die sicherheitskritischen Parameter umsetzen.
      Windows + r gpedit.msc Computerkonfiguration Windows-Einstellungen Sicherheitseinstellungen Kontorichtlinien Kennwortrichtlinien
   d. Nach zeitweiser Inaktivität der Tastatur oder Maus muss automatisch eine Bildschirmsperre aktiviert werden, die erst nach erneuter Identifikation und Authentisierung deaktiviert wird.
      Einstellungen (Windows + i) System Netzwerkbetrieb und Energiesparen
2. **Zugriffskontrolle**
   a. Der Telearbeitsrechner muss mindestens über die zwei getrennten Benutzergruppen Benutzer und Administrator verfügen.
      Der Telearbeiter soll in die Gruppe Benutzer aufgenommen werden.
      lokale Benutzer und Gruppen Gruppen oder Benutzer
   b. Mittels einer differenzierten Rechtestruktur (lesen, schreiben, ausführen, ...) muss der Zugriff auf Dateien und Programme geregelt sein.
      Rechtsklick Eigenschaften Sicherheit Bearbeiten
3. **Protokollierung**
   a. Auf dem Telearbeitsrechner sollen besondere Ereignisse automatisch protokolliert werden. Die Ergebnisse sollen in einer benutzerdefinierten Ansicht angezeigt werden.
      Windows + r eventvwr.exe Benutzerdefinierte Ansicht erstellen Protokolle: Windows-Protokolle Ereignis-IDs: 4634, 4624, 4648, 4672 (Anmeldung)
   b. Damit Unberechtigte keinen Zugriff auf die Ereignisanzeige haben oder diese manipulieren können, muss der Zugriff eingeschränkt werden.
      Windows + r REGEDIT.exe Computer HKEY_LOCAL_MACHINE SYSTEM CurrentControlSet Services EventLog Neuer Wert Datentyp: REG_DWORD Name: RestrictGuestAccess Wert: 1
4. **Verschlüsselungskomponente**
   a. Alle Laufwerke des Telearbeitsrechners müssen mit einer geeigneten Software verschlüsselt sein. Windows stellt die vorinstallierte Verschlüsselungssoftware BitLocker bereit.
      Systemsteuerung BitLocker-Laufwerksverschlüsselung BitLocker aktivieren (Anweisungen folgen)
   b. Schlüssel (auch mittlerweile nicht mehr benutzte) dürfen nie ungeschützt, das heißt auslesbar oder unverschlüsselt, abgelegt werden. Sie müssen getrennt vom verschlüsselten Gerät aufbewahrt werden.
5. **Benutzerumgebung**

a. Alle nicht benötigten Anwendungen und Komponenten müssen deaktiviert werden.
b. Programme, die der Telearbeiter nicht nutzen darf, müssen beschränkt werden. Ermöglichen kann man dies, indem man das Programm im AppLocker hinterlegt.
   lokale Sicherheitsrichtlinien Anwendungsrichtlinien AppLocker Ausführbare Regeln Rechtsklick Neue Regel erstellen verweigern Programm auswählen
c. Unerwünschte Hardware kann über den Gerätemanager blockiert werden.
   Gerätemanager Rechtsklick Gerät deaktivieren
d. Dem Telearbeiter darf es nicht möglich sein, unerlaubte Fremdsoftware auf dem Telearbeitsrechner zu installieren.
   Da die Installation von Software nur für Benutzer der Gruppe Administrator möglich ist, kann ein Telearbeiter ohne Administrator Rechte auch keine Software installieren.

6. **Virenschutz**
   a. Auf dem Telearbeitsrechner muss ein aktiviertes Computer-Viren-Prüfprogramm installiert sein.
      Als Virenschutz Sophos verwenden. Das Standard-Installationspaket kann über die Webseite der Stabsstelle Sicherheit Informationstechnischer Systeme (ST-SIS) heruntergeladen werden.
   b. Vor dem Einspielen von Daten von auswechselbaren Datenträgern, vor der Weitergabe von Datenträgern beziehungsweise beim Senden und Empfangen von Daten muss ein Virencheck durchgeführt werden.
      Rechtsklick auf die zu überprüfende Datei oder den Ordner Mit Sophos Anti-Virus überprüfen
7. **Fernwartung (Remote Administration)**
   a. Zur Fernwartung ist das Online-Fernhilfe-Tool ISL Light 4 zu nutzen. Dabei ist darauf zu achten, dass die Fernadministration nur durch autorisierte Supportmitarbeiter (Administratoren) der FSU Jena durchzuführen ist.
8. **VPN Verbindung**
   a. Für eine sichere Kommunikation zwischen dem Telearbeitsrechner und dem internen Universitätsnetz kommt eine VPN-Verbindung zum Einsatz.
      Um eine VPN-Verbindung aufzubauen, steht die Software Cisco AnyConnect Client zur Verfügung.
   b. Damit die Kommunikation nachvollziehbar ist, wird die VPN-Verbindung in der Ereignisanzeige protokolliert.
      Relevante Ereignis-IDs für die Filterung sind: 3020, 2085, 2084.
9. **Datensicherung**
   a. Bei der Datensicherung auf externen Festplatten ist darauf zu achten, dass die Backup-Datenträger verschlossen aufbewahrt werden. Zusätzlich muss der externe Datenträger verschlüsselt sein.
      Systemsteuerung BitLocker-Laufwerksverschlüsselung BitLocker aktivieren (Anweisungen folgen)
   b. Die Daten sollten außerdem in der Cloud gesichert werden, damit die Daten bei Verlust des Telearbeitsrechners erhalten bleiben.
10. **Power Shell**
    a. Die Richtungseinstellung: "Lokale Skripts und remote signierte Skripts zulassen" muss aktiviert werden.
       Dadurch werden alle lokalen Skripts zur Ausführung zugelassen.
       Skripts aus dem Internet müssen von einem vertrauenswürdigen Herausgeber signiert sein.
       Windows + r gpedit.msc Computerkonfiguration Administrative Vorlagen Windows-Komponenten Windows Power Shell Skriptausführung aktivieren aktivieren Ausführungsrichtlinie Lokale Skripts und remote signierte Skripts zulassen
11. **Firewall**
    a. Die Firewall muss auf dem Telearbeitsrechner aktiviert sein.
       Systemsteuerung System und Sicherheit Windows Defender Firewall Windows Defender Firewall ein- oder ausschalten