Sicherheitsrichtlinien für Telearbeitsplätze (Mac OS)

Zusammenfassung

Auf dieser Seiten sind Informationen zu folgenden Themen zu finden:

- Checkliste
- Umsetzungshinweise

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	
		Kontosperrdauer: 30 Minuten	
		Zurücksetzungsdauer des Kontosperrungszählers: 30 Minuten	
Kennwortrichtlinien			
		mindestens 12 Zeichen	
		das Passwort darf noch nie verwendet worden sein	
	Bildschirmsperre nach 10 Minuten Abwesenheit		
2. Zugriffskontrolle			
	mindestens zwei Benutzergruppen (Administrator und Telearbeiter)	Systemeinstellungen Benutzer & Gruppen Schloss zum entsperren "+" Symbol	
	Rechteverteilung	Rechtsklick auf Ordner oder Datei Informationen Freigabe & Zugriffsrechte	
		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	Finder Programme Dienstprogramme Aktivitätsanzeige Rechtsklick Informationen Freigabe & Zugriffsrechte	
4. Verschlüsselungskomponente			
	alle Laufwerke sind verschlüsselt	Systemeinstellungen Sicherheit Schloss zum entsperren FileVault aktivieren	
	Schlüssel nicht unverschlüsselt gespeichert		
5. Benutzerumgebung			
	nicht benötigte Anwendungen und Komponenten deaktiviert	Programme Rechtsklick in den Papierkorb legen	

	Zugriff auf spezielle Programme für Telearbeiter eingeschränkt	Finder Programme Rechtsklick auf Programm Informationen Freigabe & Zugriffsrechte
	unerwünschte Hardware blockiert	Menü "Apple" "Über diesen Mac" Weitere Informationen Systembericht
	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. Firewall		
	Firewall aktiviert	Systemeinstellungen Sicherheit Firewall Schloss zum entsperren Firewall aktivieren

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.
    c. Vorgaben für die sicherheitskritischen Parameter umsetzen.
    d. Nach zeitweiser Inaktivität der Tastatur oder Maus muss automatisch eine Bildschirmsperre aktiviert werden, die erst nach erneuter Identifikation und Authentisierung deaktiviert wird.
    Systemeinstellungen Energie sparen Ruhezustand für Computer
2. **Zugriffskontrolle**
    a. Der Telearbeitsrechner muss mindestens über die zwei getrennten Benutzergruppen Benutzer und Administrator verfügen.
    Der Telearbeiter soll in die Gruppe Standard aufgenommen werden.
    Systemeinstellungen Benutzer & Gruppen Schloss zum entsperren "+" Symbol
    b. Mittels einer differenzierten Rechtestruktur (lesen, schreiben, ausführen, ...) muss der Zugriff auf Dateien und Programme geregelt sein.
    Rechtsklick auf Ordner oder Datei Informationen Freigabe & Zugriffsrechte
3. **Protokollierung**
    a. Auf dem Telearbeitsrechner sollen besondere Ereignisse automatisch protokolliert werden. Die Ergebnisse sollen in einer benutzerdefinierten Ansicht angezeigt werden.
    Konsole
    b. Damit Unberechtigte keinen Zugriff auf die Ereignisanzeige haben oder diese manipulieren können, muss der Zugriff eingeschränkt werden.
    Finder Programme Dienstprogramme Aktivitätsanzeige Rechtsklick Informationen Freigabe & Zugriffsrechte
4. **Verschlüsselungskomponente**
    a. Alle Laufwerke des Telearbeitsrechners müssen mit einer geeigneten Software verschlüsselt sein. Windows stellt die vorinstallierte Verschlüsselungssoftware FileVault bereit.
    Systemeinstellungen Sicherheit Schloss zum entsperren FileVault aktivieren
    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.
    Programme Rechtsklick in den Papierkorb legen
    b. Programme, die der Telearbeiter nicht nutzen darf, müssen beschränkt werden.
    Finder Programme Rechtsklick auf Programm Informationen Freigabe & Zugriffsrechte
    c. Unerwünschte Hardware kann über den Gerätemanager blockiert werden.
    Menü "Apple" "Über diesen Mac" Weitere Informationen Systembericht
    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.
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.
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.
   b. Die Daten sollten außerdem in der Cloud gesichert werden, damit die Daten bei Verlust des Telearbeitsrechners erhalten bleiben.
10. **Firewall**
    a. Die Firewall muss auf dem Telearbeitsrechner aktiviert sein.
    Systemeinstellungen Sicherheit Firewall Schloss zum entsperren Firewall aktivieren