**Detaillierte Maßnahmen zur Sicherung von Hardwareobjekten im Home-Office**

**Laptop**

* **Verschlüsselung**:
  + - Verwenden von Full-Disk-Encryption (z.B. BitLocker, FileVault) zur Sicherung aller gespeicherten Daten.
    - Einrichten einer TPM (Trusted Platform Module) für zusätzliche Sicherheit.
* **Regelmäßige Backups**:
* Nutzung von Cloud-Backup-Diensten (z.B. Google Drive, OneDrive) oder lokalen Backup-Lösungen (z.B. externe Festplatten).
* **Zugangskontrolle**:
* Einrichtung von Benutzerkonten mit starken Passwörtern.
* Nutzung von biometrischen Authentifizierungsmethoden (z.B. Fingerabdruck, Gesichtserkennung).

**Smartphone**

* **Mobile Device Management (MDM)**:
  + Implementierung einer MDM-Lösung (z.B. Microsoft Intune, MobileIron) zur Verwaltung und Überwachung mobiler Geräte.
* **Verschlüsselung**:
  + - Aktivierung der Geräteeinstellungen zur Datenverschlüsselung (z.B. Android-und iOS-Geräte bieten eingebaute Verschlüsselungsfunktionen).

**Zwei-Faktor-Authentifizierung**:

* Nutzung von 2FA-Apps (z.B. Google Authenticator, Authy) oder SMS-basierter 2FA für zusätzliche Sicherheit bei der Anmeldung.

**Drucker/Scanner**

* **Sichere Netzwerkverbindung**:
* Verbindung über ein sicheres WLAN mit WPA3-Verschlüsselung.
* Verwendung eines VPN für den Zugang zu Unternehmensnetzwerken.
* **Benutzerauthentifizierung**:
* Einrichtung von Benutzerkonten und PINs zur Nutzung desDruckers/Scanners.
* Implementierung von Druckaufträgen nur nach Authentifizierung des Benutzers.

**Externe Festplatte**

* **Verschlüsselung**:
* Einsatz von Hardware-verschlüsselten Festplatten (z.B. IronKey, Kingston).
* Nutzung von Software-Verschlüsselungstools (z.B. VeraCrypt) zur Sicherung der Daten.
* **Regelmäßige Backups**:
* Erstellung automatischer Backup-Routinen (z.B. wöchentliche Backups) mit Backup-Software (z.B. Acronis True Image, Macrium Reflect).
* **Physischer Schutz**:
* Aufbewahrung der Festplatte in einem sicheren, abschließbaren Schrank.
* Verwendung von Kensington-Schlössern zur Sicherung der Festplatte gegen Diebstahl.

**WLAN-Router**

* **Sichere Konfiguration**:
  + Änderung des Standard-Admin-Passworts.
  + Deaktivierung von WPS (Wi-Fi Protected Setup).
  + Aktivierung von WPA3-Verschlüsselung für das WLAN.
* **Firmware-Updates**:
  + Regelmäßige Überprüfung und Installation von Firmware-Updates vom Hersteller.
  + Aktivierung von automatischen Updates, falls verfügbar.
* **Starke Passwörter**:
  + Verwendung eines komplexen und einzigartigen Passworts für das WLAN.
  + Erstellung eines separaten Gastnetzwerks mit eigenem Passwort für Besucher.

**USB-Sticks**

* **Verschlüsselung**:
  + Einsatz von verschlüsselten USB-Sticks (z.B. SanDisk SecureAccess, Kingston DataTraveler).
  + Nutzung von Softwarelösungen zur Verschlüsselung der Daten auf dem Stick (z.B. BitLocker To Go).
* **Verwendung von sicheren USB-Sticks**:
  + Auswahl von USB-Sticks mit zusätzlichen Sicherheitsfeatures wie Passwortschutz oder Fingerabdruckscanner.

**Docking Station**

* **Physischer Schutz**:
  + Sicherung der Docking Station an einem festen Ort, z.B. durch Kensington-Schlösser.
* **Zugangskontrolle**:
  + Begrenzung des Zugriffs auf die Docking Station nur auf autorisierte Benutzer durch Passwörter oder biometrische Authentifizierung.