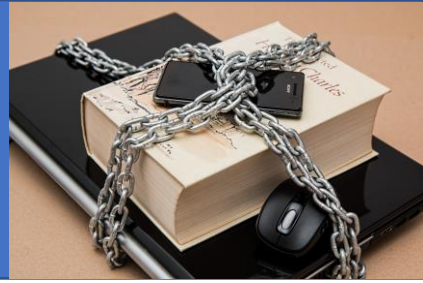
DIGITAL SECURITY CHECKLISTE

Checkliste zum ausdrucken

Frank-Hilft.de



Verwendung der **Security-Checkliste**

- *Jede Checkbox ist ein eigener Punkt*
- *Prüfen Sie die einzelnen Punkte ob diese in Ihrer Umgebung zutreffen und kreuzen Sie die erledigten Punkte ab, wenn Sie abgeschlossen sind*

Router Sicherheit

System Sicherheit

- ❑ 1. Verwende einen individuellen „selbst erstellten“ administrativen Benutzer (Account) und deaktiviere das Konto **Admin** und das **Konto** Gast
- ❑ 2. Schalten Sie die 2 Faktor-Authentifizierung ein
- ❑ 3. Ändern Sie die Default Ports, z.B. 80, oder 443 für die Management-Webseite des Routers
- ❑ 4. Aktivieren Sie die IP Autoblock-Funktion für Brut-Force Angriffe
- ❑ 5. Verwenden Sie HTTPS mit einem gültigen Zertifikat
- ❑ 6. Konfigurieren Sie Push, SMS oder E-Mail Benachrichtigungen um über kritische Ereignisse informiert zu werden
- ❑ 7. Aktivieren Sie die automatische Aktualisierungsfunktion um die Firmware stets aktuell zu halten

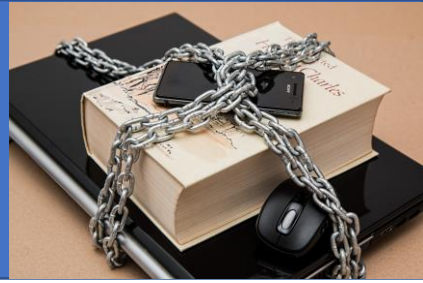
Netzwerk Sicherheit

- ❑ 8. Verwenden Sie den Zugriff auf die Roter-Administration nur im Lan oder über VPN
- ❑ 9. Synology Safe Access einschalten, um verdächtige (malicios) Domains und IP-Adressen zu sperren
- ❑ **10. Threat Protection** und **Deep Packet Inspection** aktiviren
- ❑ 11. Aktivieren Sie DNS over HTTPS Encryption zum Schutz vor DNS-hijacking
- ❑ 12. Aktivieren Sie GEO-IP Firewall-Regeln
- ❑ 13. Erstellen Sie MAC-Filter und Zugriffsregeln (Whitelist) für Ihr WiFi-Netzwerk
- ❑ 14. Verwenden Sie ein GAST –WiFi-Netzwerk mit einem eignen Netzwerksegment (unterschiedliche IP-Adressen)
- ❑ 15. Aktivieren Sie einen Zeitplan für Traffic-Reports

DIGITAL SECURITY CHECKLISTE

Checkliste zum ausdrucken

Frank-Hilft.de



Verwendung der **Security-Checkliste**

- *Jede Checkbox ist ein eigener Punkt*
- *Prüfen Sie die einzelnen Punkte ob diese in Ihrer Umgebung zutreffen und kreuzen Sie die erledigten Punkte ab, wenn Sie abgeschlossen sind*

NAS Sicherheit

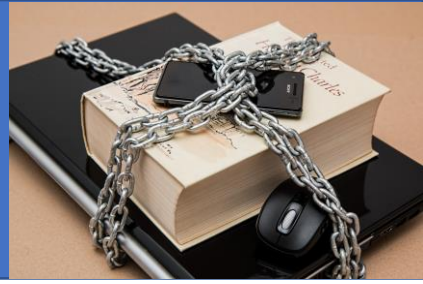
System Sicherheit

- ❑ 1. Verwende ein individuelles „selbst erstelltes“ administratives Konto (Account) und deaktivieren das Konto **Admin**
- ❑ 2. Aktivieren Sie **die 2 Faktor-Authentifizierung** für alle Benutzer
- ❑ 3. Ändern Sie die Default Ports 5000 und 5001 für die Zugriff auf die DSM-Management Konsole
- ❑ 4. Erstellen Sie eine „strenge Passwortrichtline“ mit „straken Passwort“ für die NAS-Benutzer
- ❑ 5. Deaktivieren Sie nicht erforderliche Dienste u. Protokolle
- ❑ 6. Begrenzen Sie den Zugriff auf verwendete Dienste und Protokolle
- ❑ 7. Begrenzen Sie den Zugriff auf Gemeinsame Ordner und definieren Sie die individuellen Berechtigungen
- ❑ 8. Verwenden Sie für Anwendungen HTTPS mit einem gültigen SSL Zertifikat
- ❑ 9. Konfigurieren Sie Push oder E-Mail Benachrichtigungen um den Administrator über Warnung und kritische Ereignisse zu informieren
- ❑ 10. Ändern Sie bei Portforwarding-Regeln die Standard-Ports 5000/5001 in eigene verfügbare Ports. (z.B. 55000 ect.)
- ❑ 11. Aktivieren Sie die IP Autoblock-Funktion für Brut-Force Angriffe
- ❑ 12. Aktivieren Sie HTTPS für den Zugriff auf DSM mit einem gültigen SSL-Zertifikat (z.B. von Lets encrypt)
- ❑ 13. Threat Protection und Deep Packet Inspection aktivieren
- ❑ 14. Aktivieren Sie die automatische Aktualisierung von DSM
- ❑ 15. Aktivieren Sie die automatische Aktualisierung von Synology-Paketen
- ❑ 16. Erstellen Sie Anwendungs- und GEO-IP Firewall-Regeln
- ❑ 17. Installieren Sie das Antivirus Paket und erstellen Sie einen Zeitplan für einen regelmäßigen Scan
- ❑ 18. Verwenden Sie ein GAST –WiFi-Netzwerk mit einem eignen Netzwerksegment (unterschiedliche IP-Adressen)
- ❑ 19. Aktivieren Sie einen Zeitplan für Traffic-Reports

DIGITAL SECURITY CHECKLISTE

Checkliste zum ausdrucken

Frank-Hilft.de



Verwendung der **Security-Checkliste**

- *Jede Checkbox ist ein eigener Punkt*
- *Prüfen Sie die einzelnen Punkte ob diese in Ihrer Umgebung zutreffen und kreuzen Sie die erledigten Punkte ab, wenn Sie abgeschlossen sind*

Daten Sicherheit/Backup

Computer / Notebook

- ❑ 1. Verwenden Sie **Synology Drive** für die Sicherung von wichtigen Daten
- ❑ 2. Verwenden Sie **Active Backup for Business** für die Imagebasierte (Komplett) Sicherung von Server, PC und Synology DSM 7.x
- ❑ 3. Windows-PC: Aktivieren Sie die „**Dateiversionsverlauf**-Sicherung“ für die schnelle Wiederherstellung von persönlichen Daten
- ❑ 4. macOS: Aktivieren Sie die Funktion Time Machine Backup

NAS Synology Backup

- ❑ 1. Verwenden Sie **Hyper-Backup** für die Sicherung von Dateien, Gemeinsame Ordner, LUNs und Anwendungseinstellungen
- ❑ 2. Aktivieren Sie Snapshots für wichtige Datenfreigaben für eine schnellere Wiederherstellung
- ❑ 3. Verwenden Sie die Benachrichtigungen um sich über fehlerhafte Datensicherungs-Aufgaben zeitnah zu informieren
- ❑ 4. Erstellen Sie mit Hyper-Backup eine Sicherungsaufgabe für eine lokale Sicherung auf eine andere NAS, oder ein USB-Laufwerk
- ❑ 5. Erstellen Sie einen weiteren Sicherungsplan für Ihre wichtigen Daten und legen Sie ein externes Ziel fest (z.B. C2-Cloud o.ä.)

USB-Geräte

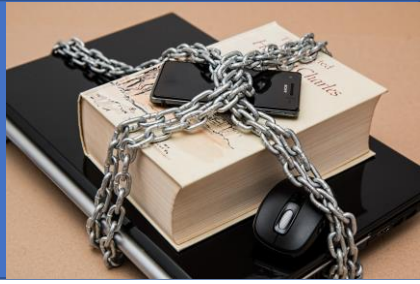
- ❑ 1. Verwenden Sie USB-Copy für eine Sicherung Ihrer Daten auf ein externes Laufwerk. (z.B. USB-Festplatte)
- ❑ 2. Nutzen Sie für die Datensicherung keinen USB-Stick. USB Festplatten sind deutlich robuster und gehen auch nicht so leicht verloren
- ❑ 3. Überprüfen Sie in regelmäßigen Abständen den Erfolg Ihrer Datensicherung und führen Sie testweise eine Wiederherstellung der gesicherten Daten aus

Backup Regeln

- ❑ 1. Erstellen Sie einen automatischen Sicherungszeitplan, der regelmäßig die wichtigen Datenselbstständig sichert
- ❑ 2. Verwenden Sie 2 oder mehr USB-Laufwerke oder ein zusätzliches Sicherungsziel (z.B. DiskStation) außerhalb Ihres Gebäudes auf
- ❑ 3. Bewahren Sie ein USB-Backup an einem anderen physischen Ort auf
- 4. Nutzen Sie als Sicherungsziel zusätzlich einen entfernten Standort oder eine Cloud-Lösung (z.B. Synology C2 Cloud

DIGITAL SECURITY CHECKLISTE

Frank-Hilft.de



Empfehlungen & Lernpfade

Sicherheit

Video-Tpp
11 Sicherheit-Tipps für die Synology
Sicherheitsrelevante Einstellungen für den externen Zugang

Video ansehen

Video-Tpp
Secure Sign In App Anmeldung auch ohne Passwort

Video ansehen

Lern-Tpp
Online-Training DSM 7 von A-Z (Kompendium)

Online-Training ansehen

Lern-Tpp
Online-Support-Coaching mit Frank

Informationen ansehen

SYNOLOGY
Support-Coaching

Datensicherung

Video-Tpp
Playlist zum Thema Datensicherung

Playlist ansehen

Lern-Tpp
Online-Kurs: Active Backup for Business

Online-Kurs ansehen

Lern-Tpp
Online-Kurs: Hyper Backup Grundlagen

Online-Kurs ansehen

Lern-Tpp
Online-Kurs: Bitwarden auf Synology installieren

Online-Kurs ansehen