DIGITAL SECURITY CHECKLIST

Die Anzahl der vernetzten Geräte nimmt stetig zu. Damit wird es auch für Cyber-Angreifer immer einfacher, schwache Sicherheitspraktiken des Netzwerks zu identifizieren, auszunutzen und sich Zugang zu kritischen Daten zu verschaffen. Prüfen Sie Ihr Netzwerk mit dieser Checkliste. Sehen Sie auf einem Blick, was Sie bereits gut schützen und wo Sie noch Verbesserungspotential haben.

Gehen Sie dafür Schritt für Schritt alle wichtigen Sicherheitspunkte durch. Jedes angekreuzte Kontrollkästchen entspricht einem Punkt. Je mehr Punkte Sie haben, um so besser sind Ihre Daten und Geräte geschützt. Insgesamt können Sie 44 Punkte erreichen.

Schutz für PC & Mobilgeräte

Punkte /4

- ☐ Halten Sie Ihr Betriebssystem auf dem neuesten Stand
- ☐ Installieren Sie eine zuverlässige Antivirensoftware und führen Sie regelmäßig vollständige Scans durch
- ☐ Aktivieren Sie das Remote Desktop Protocol (RDP) nur, wenn der Fernzugriff unbedingt erforderlich ist, um Sie vor Angriffen, die dieses Protokoll ausnutzen, zu schützen
- ☐ Wenn Sie öffentliches WLAN verwenden, verschlüsseln Sie die Verbindung immer mit einer VPN-Verbindung

Schutz für IoT-Geräte

Punkte /4

- ☐ Verwenden Sie ein starkes Passwort
- ☐ Sperren Sie Geräte (z. B. IP-Kameras, Drucker, Telefone usw.) vom Zugriff auf das Internet, es sei denn, die Gerät benötigt eine Kommunikation mit einem Internet-Server, um zu funktionieren
- ☐ Verbinden Sie IoT-Geräte mit dem Gastnetzwerk und trennen Sie sie von benutzereigenen Geräten wie Computern, Smartphones und NAS, um zu verhindern, dass ein IoT-Gerät gekapert wird und andere Geräte im selben Netzwerk angreift
- ☐ Blockieren Sie ein Gerät sofort, wenn es Anzeichen verdächtiger Aktivitäten zeigt. Untersuchen Sie die Vorfälle und setzen Sie das Gerät bei Bedarf zurück/installieren Sie es neu

Schutz für NAS

Punkte /12

- ☐ Verwenden Sie ein benutzerdefiniertes Administratorkonto und deaktivieren Sie die Standardkonten „admin“ und „guest“
- ☐ Aktivieren Sie die 2-Stufen-Authentifizierung
- ☐ Wenden Sie starke Regeln für die Passwortstärke auf alle Ihre Benutzer an
- ☐ Beschränken Sie die Zugriffsrechte der Benutzer auf die freigegebenen Ordner und Dienste, die sie nicht benötigen
- ☐ Ändern Sie die Standardports des Systems, z. B. Port 5000/5001 für die Verwaltungsschnittstelle des NAS Betriebssystems (DiskStation Manager, kurz DSM) auf neue benutzerdefinierte Ports im höheren 5-stelligen Bereich.
- ☐ Wenn die Portweiterleitung für Ihr NAS aktiviert ist, verwenden Sie statt bekannter Ports (z. B. 5000/5001) benutzerdefinierte öffentliche Ports auf dem Router
- ☐ Aktivieren Sie die automatische IP-Blockierung gegen Brute-Force-Angriffe
- ☐ Aktivieren Sie HTTPS für Dienste, die auf DSM mit einem gültigen SSL-Zertifikat ausgeführt werden
- ☐ Aktivieren Sie E-Mail-, SMS- oder Push-Benachrichtigungen, um über kritische Ereignisse auf dem Laufenden zu bleiben
- ☐ Aktivieren Sie die automatische Aktualisierung für DSM
- ☐ Führen Sie den Security Advisor regelmäßig aus, um Systemschwachstellen aufzudecken und Malware zu identifizieren
- ☐ Installieren Sie ein Antivirenpaket und führen Sie regelmäßig vollständige Scans durch

Perimeter-Schutz für Router

Punkte /14

System Security

- ☐ Verwenden Sie ein benutzerdefiniertes Administratorkonto und deaktivieren Sie die Standardkonten „admin“ und „guest“.
- ☐ Aktivieren Sie die 2-Stufen-Authentifizierung
- ☐ Ändern Sie die Standardports des Systems, z.B Port 8000/8001 der Verwaltungsschnittstelle auf neue benutzerdefinierte Ports, wenn Sie Synology Router Manager (SRM) verwenden
- ☐ Aktivieren Sie die automatische IP-Blockierung gegen Brute-Force-Angriffe
- ☐ Aktivieren Sie HTTPS für Dienste, die auf SRM mit einem gültigen SSL-Zertifikat ausgeführt werden
- ☐ Aktivieren Sie E-Mail-, SMS- oder Push-Benachrichtigungen, um über kritische Ereignisse auf dem Laufenden zu bleiben
- ☐ Aktivieren Sie die automatische Aktualisierung der Router-Firmware und aller integrierten Sicherheitsdatenbanken

Network Security

- ☐ Greifen Sie über VPN auf Geräte im Büro oder Zuhause zu
- ☐ Aktivieren Sie Synology Safe Access, um schädliche Domänen und IP-Adressen zu blockieren
- ☐ Aktivieren Sie Threat Prevention und Deep Packet Inspection
- ☐ Aktivieren Sie die DNS-über-HTTPS-Verschlüsselung, um DNS-Hijacking zu verhindern
- ☐ Aktivieren Sie GeoIP-Firewallregeln
- ☐ Aktivieren Sie die Mac-Filterung und die Whitelist bekannter Geräte für die WLAN-Nutzung
- ☐ Aktivieren Sie regelmäßig geplante Traffic-Berichte, um die Netzwerknutzung zu überwachen

Datenschutz mit Backup

Punkte /10

Backup des PCs

- ☐ Aktivieren Sie Synology Drive, um wichtige Dateien und Ordner zu sichern
- ☐ Aktivieren Sie Active Backup for Business, um das gesamte System zu sichern

Backup des NAS

- ☐ Aktivieren Sie Hyper Backup, um freigegebene Ordner, LUNs und System-/Paketkonfigurationen zu sichern
- ☐ Konfigurieren Sie in Hyper Backup eine Warnschwelle für Dateiänderungen zwischen zwei Sicherungsversionen, so dass Sie automatisch über abnormales Verhalten benachrichtigt werden und somit einem eventuellen Datenverlust vorbeugen können.
- ☐ Aktivieren Sie Snapshot Replication, um Snapshots wichtiger freigegebener Ordner zu erstellen
- ☐ Aktivieren Sie Cloud Sync, um Dateien und Ordner kontinuierlich bei einem sicheren öffentlichen Cloud-Anbieter wie Synology C2 Storage zu sichern

Backup externer Geräte (z.B. USB-Festplatten)

- ☐ Verwenden Sie USB Copy, um alle externen Geräte zentral zu Ihrem NAS zu sichern

Weitere wichtige Backup-Einstellungen

- ☐ Bewahren Sie mindestens eine Offsite-Kopie für die Notfallwiederherstellung auf
- ☐ Planen Sie alle Ihre Backup-Aufgaben so, dass sie automatisch ausgeführt werden
- ☐ Testen Sie nach der ersten Sicherung, ob Sie die Daten aus der Sicherungskopie wiederherstellen können. Wiederholen Sie dies anschließend regelmäßig, um sicherzustellen, dass Sie bei Ausfällen immer eine vollständige Wiederherstellung durchführen können