Bitdefender

Ihre Checkliste: Familiengeräte auf dem Prüfstand

Cybersicherheit für unterwegs (VPN)

- ☑ Installieren Sie auf möglichst vielen Geräten eine VPN-Lösung
- ☑ Wählen Sie einen bevorzugten Server an einem geografischen Standort, der die Einhaltung Ihrer lokalen Rechte bei der Datenvereinbarung gewährleistet
- ☑ Lesen Sie die Endbenutzer-Lizenzvereinbarung, um zu verstehen, welche Daten aufgezeichnet werden, wie die Daten aufbewahrt werden und welche Daten der Anbieter über Sie sammeln kann

Ein sicheres Smart Home

- ☑ Ändern Sie die Administrator-Passwörter für alle intelligenten Geräte im Haushalt
- ☑ Richten Sie ein Gastnetzwerk ein, über das fortan alle Geräte im Internet der Dinge separat laufen
- ☑ Deaktivieren Sie nicht benötigte Funktionen
- ☑ Überwachen Sie Geräte auf ungewöhnliches Verhalten (dies kann mit einem Router mit
- ☑ integrierter Sicherheit automatisiert werden)
- ☑ Sorgen Sie dafür, dass Geräte im Internet der Dinge auf dem neuesten Stand laufen und alle aktuellen Patches eingespielt wurden

Sichere Passwörter und Passwortverwaltung

- ☑ Verwenden Sie sichere alphanumerische Passwörter mit einigen Sonderzeichen (%$^#&)
- ☑ Verwenden Sie unterschiedliche Passwörter für jedes Benutzerkonto, so vermeiden Sie, dass gleich mehrere Konten von Datenpannen betroffen sind
- ☑ Aktivieren Sie auf jeder Plattform, die dies auch anbietet, die Zwei-Faktor-Authentifizierung
- ☑ Erwägen Sie die Verwendung eines Passwortmanagers, so können Passwörter bequem verwaltet und Kreditkartendaten sicher verwahrt und bei Bedarf automatisch angegeben werden

Ein sicherer Browser

- ☑ Aktualisieren Sie den Browser so werden auch gleich die neuesten Sicherheitsupdates installiert
- ☑ Legen Sie im Detail fest, welche Cookies akzeptiert werden sollen und aktivieren Sie die „Do Not Track“-Funktion
- ☑ Verwalten Sie Website-Einstellungen und Berechtigungen wie Standortverfolgung, Kamera- und Mikrofonzugriff, Benachrichtigungen und Hintergrundsynchronisierung
- ☑ Führen Sie regelmäßig die „Sicherheitsprüfung“ durch

Ein sicherer Computer

- [x] Installieren Sie die neuesten Updates
- [x] Legen Sie fest, dass zukünftige Systemupdates automatisch installiert werden sollen
- [x] Überprüfen Sie die Einstellungen für Benutzerkontensteuerung und Datenschutz und passen Sie sie bei Bedarf an
- [x] Bringen Sie den Web-Browser auf den neuesten Stand, schränken Sie die Verwendung von Browser-Erweiterungen ein und überprüfen Sie vorhandene Plug-ins und Erweiterungen
- [x] Verschlüsseln Sie die Festplatte zum Schutz bei Verlust oder Diebstahl
- [x] Installieren Sie eine Sicherheitslösung zur Abwehr bekannter und unbekannter Bedrohungen

Ein sicherer Router

- [x] Halten Sie den Router immer auf dem neuesten Stand
- [x] Ändern Sie die Standard-Anmeldedaten und verwenden Sie WPA3-Verschlüsselung
- [x] Deaktivieren Sie WSP und UPnP, wenn sie nicht unbedingt erforderlich sind
- [x] Richten Sie für Gastgeräte ein Gastnetzwerk ein
- [x] Deaktivieren Sie die webbasierte Verwaltungsoberfläche
- [x] Verwenden Sie einen VPN-Tunnel, wenn dieser von Ihrem Router unterstützt wird
- [x] Wenn das Gerät bereits veraltet ist und ersetzt werden muss, entscheiden Sie sich für ein neues Gerät mit integriertem IoT- und Endpoint-Schutz

Ein sicherer Drucker

- [x] Schränken Sie das Drucken über die Cloud ein, wenn es nicht genutzt wird
- [x] Deaktivieren Sie UpnP in Ihrem Heimnetzwerk
- [x] Legen Sie ein eigenes Passwort für den Drucker fest
- [x] Sorgen Sie dafür, dass der Drucker auf dem neuesten Stand ist
- [x] Verwenden Sie einen abgesicherten Router bzw. stellen Sie sicher, dass Ihr WLAN-Netzwerk mit einem Passwort geschützt ist

Sicheres Telefon und Tablets

- [x] Installieren Sie eine Sicherheitslösung, um Telefone und Tablets vor Malware, Phishing und betrügerischen Links zu schützen
- [x] Installieren Sie eine VPN-Lösung, um verschlüsseltes Surfen auch unterwegs zu gewährleisten, und aktiveren Sie (wenn möglich) die Option für den Dauerbetrieb
- [x] Prüfen Sie, ob auf den Geräten die neueste Version des Betriebssystems installiert ist
- [x] Regen Sie den Kauf eines neuen Geräts an, wenn das Telefonmodell nicht mehr unterstützt wird