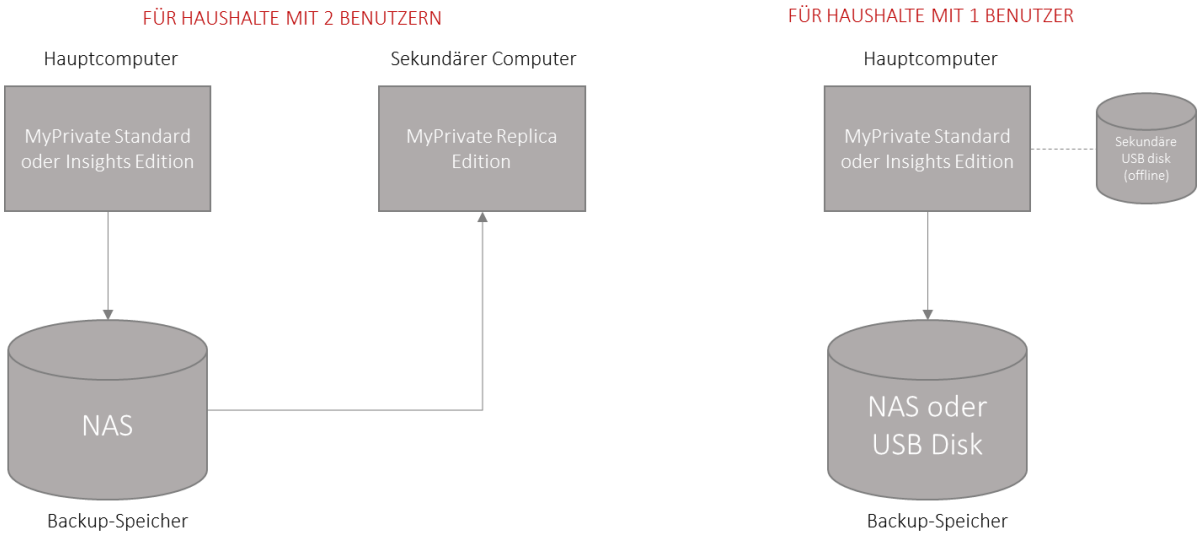
Benutzer von MyPrivate werden über die Jahre wertvolle Daten kumulieren, und es ist wichtig, die Informationen vor Verlust, Korruption oder Diebstahl zu schützen.

Es gibt zwar keine 100%-ige lückenlose Lösung, aber es gibt viele gute Praktiken, die es sehr unwahrscheinlich machen dass Diebstahl oder Datenverlust auftreten.

Die meisten MyPrivate-Haushalte haben einen oder zwei Benutzer; Die folgende minimale Hardwarekonfiguration wird für einen soliden Schutz empfohlen:



Konfigurationsempfehlungen

- Windows 10 Professional mit automatischem Download und Installation von Updates.
- Verwendung der Standard Windows Defender und Windows Firewall.
- Verwendung eines VPNs, wenn man mit einem externen Netzwerk wie einem Café, Hotel oder Flughafen verbunden ist.
- Datenverschlüsselung Ihrer Laufwerke; Für den Hauptcomputer, den sekundären Computer und die USB-Geräte kann die native Windows-Bitlocker-Funktionalität verwendet werden, während der Anbieter von das NAS-Laufwerk Verschlüsselungsunterstützung bereitstellen muss. Im Falle eines Diebstahls des Computers, NAS oder USB-Festplattenlaufwerks sind die Daten nicht lesbar.
- Für Haushalte mit 1 Benutzer
    - Zusätzlich zu der Sicherung auf NAS- oder USB-Festplatten ist für monatliche Sicherungen eine separate Offline-USB-Festplatte erforderlich, die die native MyPrivate-Sicherungsfunktion verwendet. Im Falle einer Infektion mit Ransomware des Hauptcomputers und / oder NAS bleibt der Offlinespeicher intakt.

- Für Haushalte mit 2 Benutzern
    - Keine Windows-Dateifreigabe zwischen primären und sekundären Computern; Dies gewährleistet den Schutz im Falle einer Infektion mit Ransomware entweder von einem Computer und / oder dem NAS.
    - Aktivierung des Windows-Dateiversionss auf dem Hauptcomputer mit täglicher Aktualisierungshäufigkeit; Zusätzlich wird die native MyPrivate-Sicherung mit wöchentlicher Häufigkeit aktiviert. Mehrere Wiederherstellungsoptionen sind weiterhin verfügbar, wenn Datenträger oder Datenbank von einem Computer oder einem NAS beschädigt werden.
- Der Hauptcomputer, der Sekundärcomputer, der NAS und die USB-Festplatte sollten niemals physisch am gleichen Ort verbleiben, um vor Diebstahl, Wasser- oder Feuerschaden zu schützen.
- Konfiguration des Webbrowsers mit vordefinierten Links zu üblichen Links wie Finanzinstituten, wodurch das Risiko, ein Phishing-Opfer zu werden, reduziert wird.
- Aktivierung eines passwortgeschützten Bildschirmschoners mit kurzem Timeout, der vor unbefugtem Zugriff an öffentlichen Orten schützt.
- Sorgfältiges Lesen der Richtlinien für die Eingabe und Verwaltung von Codes im Modul [Familie].
- Keine Verwendung von Cloud-Speicherfunktionen wie OneDrive, DropBox zum Speichern von MyPrivate-Daten.
- USB-Schlüssel sollten nicht an einem Computer angeschlossen werden, sofern sie nicht von einem vertrauenswürdigen Ursprung stammen; es gibt bekannte Fälle von USB-Sticks, die mit Viren und / oder Ransomware infiziert sind.