Sync+Share (Nextcloud) Sicherheitsempfehlungen

Mit den hier aufgeführten Punkten wollen wir Ihnen grundlegende Empfehlungen an die Hand geben, um die Nutzung des Dienstes Sync+Share (Nextcloud) möglichst sicher zu gestalten. Weiterhin wollen wir Sie speziell für das Thema „verantwortungsvoller Umgang mit Daten“ sensibilisieren, da neben der Sicherheit des Dienstes und der gespeicherten Daten selbst, wofür das ZKI nach besten Kräften sorgt, Ihr Verhalten gerade in Hinblick auf das Teilen von Daten mit anderen Personen zu einem großen Teil zur Gesamtsicherheit beiträgt.

1. Lassen Sie bei der Nutzung des Dienstes Sync+Share (Nextcloud) Sorgfalt walten! Das persönliche Verhalten ist oft wichtiger als jede Technik.

2. Speichern Sie kein Passwort im Web-Browser ab!

3. Nutzen Sie nach Möglichkeit den „privaten Modus“ der Web-Browser bzw. löschen Sie den Browserverlauf nach getaner Arbeit. Insbesondere, wenn Sie an öffentlich zugänglichen Rechnern arbeiten.

4. Ändern Sie Ihr Passwort regelmäßig! Wir empfehlen, das Passwort mindestens jährlich zu ändern. Verwenden Sie bitte ausschließlich sichere Passwörter, sodass niemand durch "einfaches Erraten" Ihres Passwortes Ihren Account missbrauchen kann!

5. Prüfen Sie regelmäßig, ob Ihre Einladungen und Links noch „aktuell“ sind! Nicht mehr benötigte Einladungen und Links sollten entfernt werden.

6. Schränken Sie beim Einladen anderer Nutzer auf einen Ihrer Ordner die Zugriffsberechtigungen so weit als möglich ein (z.B. nur lesender Zugriff)!

7. Versehen Sie Links mit einem Ablaufdatum und/oder mit einem Passwort!

8. Versuchen Sie stets bei Einladungen und Links, den Umfang der geteilten Daten so gering wie möglich zu halten! Geben Sie nicht aus Bequemlichkeit einen größeren Umfang als unbedingt nötig frei! Legen Sie ggf. einen neuen Ordner an, um ausgewählte Daten zu teilen!

9. Prüfen Sie vor dem Einladen oder Teilen von Daten, ob auch wirklich der richtige Empfänger eingegeben wurde! Bedenken Sie, dass das versehentliche Teilen von (sensiblen) Daten möglicherweise nicht mehr rückgängig gemacht werden kann, sobald diese einmal von einem anderen Nutzer heruntergeladen wurden!

10. Denken Sie daran, dass zu ihrem Ordner eingeladene Personen Daten auf ihr eigenes System synchronisieren und lokal speichern können und somit auch nach der Entfernung der Einladung über die lokal gespeicherten Daten noch verfügen können!

11. Beachten Sie, dass personenbezogene Daten höhere Sicherheitsanforderungen haben! Verschlüsseln Sie grundsätzlich sensible Daten! Es gibt eine Reihe von geeigneten Verschlüsselungstools, z.B. BoxCryptor.

12. Posten Sie keine Links in soziale Netzwerke, da sich der Nutzerkreis unkontrolliert und stark ausweiten kann! Wenn Sie das bewusst dennoch tun möchten, dann versehen Sie bitte den Link mit einem Ablaufdatum und/oder mit einem Passwort!

13. Beachten Sie die Gefahr der Verteilung von Schadsoftware, Krypto-Trojaner oder Malware-infizierter Dateien!
    Es wird empfohlen, eine dezentrale Virenprüfung auf dem lokalen Gerät mittels einer geeigneten AntiViren-Software durchzuführen. Es wird ausdrücklich darauf hingewiesen, dass eine zentrale Virenprüfung am ZKI nicht stattfindet.

14. Ihr Rechner sollte keine bekannten Schwachstellen besitzen. Nutzen Sie deshalb den (automatischen) Update-Mechanismus Ihres Betriebssystems bzw. des Web-Browsers, durch den derartige Lücken möglichst schnell geschlossen werden.

15. Beachten Sie die Benutzerrichtlinien des Dienstes Sync+Share (Nextcloud).

Allgemeine Sicherheitshinweise zum System selbst:

1. Der Dienst Sync+Share (Nextcloud) unterliegt dem deutschen Datenschutzgesetz.

2. Ihre Daten liegen ausschließlich auf Speichersystemen in den Serverräumen des ZKI, zu denen nur ein sehr eingeschränkter Personenkreis Zugang hat. Die Räume sind voll klimatisiert und mit optimalen Brandschutzvorkehrungen ausgestattet.

3. Die Kommunikation zwischen Ihren Endgeräten und der Dienstinfrastruktur des ZKI erfolgt verschlüsselt.

4. Das ZKI trifft angemessene Vorsichtsmaßnahmen, dass die Sicherheit und Unversehrtheit der Daten gewahrt wird.

5. Das ZKI sorgt mit den ihm zur Verfügung stehenden Mitteln dafür, dass kein unberechtigter Zugriff von außen auf die im Speichersystem liegenden Daten möglich ist.