

Sicherheit & Datenschutz bei SYNCING.NET



"Datenschutz und Sicherheit stehen bei SYNCING.NET an erster Stelle. Daher haben wir umfassende Maßnahmen ergriffen, um die Sicherheit Ihrer Daten zu gewährleisten."

Unsere Sicherheitsrichtlinie beinhaltet die folgenden Komponenten um unseren Kunden höchste Sicherheit beim Austausch ihrer wertvollen Daten mit SYNCING.NET zu garantieren.

- Sicherheit im Rechenzentrum
- Netzwerksicherheit
- Benutzersicherheit
- Datenschutz

Sicherheit im Rechenzentrum

Unser Rechenzentrum mit Sitz in Berlin wurde als sicherer Standort für die geschäftskritischen Anwendungen unserer Kunden konzipiert. Betreiber des Rechenzentrums ist T-Systems, eine Tochter der Deutschen Telekom AG.

Unsere Serversysteme sind vollständig redundant ausgelegt und verwenden die hoch verlässliche MySQL-Datenbankreplikation, um die Daten zwischen den Servern abzugleichen.

Leistungsdaten:

- 100% USV-gesicherte Stromversorgung
- redundante Gigabit-Anbindung an 3 verschiedene Träger
- redundante Dieselgeneratoren
- redundante Datenbank
- 24/7 Videoüberwachung

Netzwerksicherheit

Verschlüsselung

SYNCING.NET verschlüsselt vor der Übertragung alle Daten, die in einem Sync-Ordner bzw. einer Outlook-Gruppe (Dateien oder Outlook-Elemente) ausgetauscht werden, in einem mehrstufigen Verfahren: Die Daten (Dateien oder Outlook-Elemente) werden durch individuelle 256-Bit-AES-Schlüssel verschlüsselt. Die sonstige Kommunikation (Metadaten, Austausch der AES-Schlüssel) zwischen den Teilnehmern wird wiederum in einem hochsicheren 1024-Bit-RSA-Verfahren (Private-Public-Key-Verfahren) verschlüsselt.

Authentifizierung und Verschlüsselungsdetails

Am Anfang einer Übertragung signiert der sendende PC (Peer A) den Header eines speziellen Authentifizierungs-Datenpakets mit seinem privaten 1024-Bit-RSA-Schlüssel und verschlüsselt diesen schließlich mit dem öffentlichen Schlüssel des adressierten Empfängers. Das Datenpaket wird dann an den Kommunikationspartner - einen anderen Computer (Peer B) oder den Server - gesendet. Peer B kann den Header mit dem eigenen privaten RSA-Schlüssel entschlüsseln und mithilfe des öffentlichen Schlüssels von Peer A die Echtheit des signierten Headers überprüfen (z. B. auf evtl. Manipulationen während der Übertragung). Die öffentlichen Schlüssel befinden sich auf dem Server und können von allen Mitgliedern/Peers des selben Netzwerks abgerufen werden.

Nachdem überprüft wurde, dass die Verbindung tatsächlich von einem berechtigten Computer kommt (Nachrichten unbekanntem Ursprungs werden einfach verworfen), sendet Peer B einen 256-Bit-AES-Sitzungsschlüssel an Peer A. Der Sitzungsschlüssel wird ebenfalls RSA-verschlüsselt übertragen, wobei der öffentliche Schlüssel von Peer A für die Verschlüsselung verwendet wird. Sollte zufällig ein unberechtigter Computer diese Daten abfangen wollen (eine sog. Man-in-the-middle-Attacke), kann dieser ohne den privaten Schlüssel des echten Empfängers die RSA-verschlüsselten Daten nicht entschlüsseln und damit an den Sitzungsschlüssel gelangen.

Dies ist deshalb wichtig, da alle Daten, die während der folgenden Sitzung zw. beiden Computern übertragen werden, mit diesem 256-Bit-AES-Sitzungsschlüssel ver- und entschlüsselt werden (eine sogenannte End-to-End-Verschlüsselung). Der Schlüssel ist nur bis zum Ende der jeweiligen Übertragungssitzung gültig. Jede weitere Sitzung verwendet einen anderen Schlüssel, der wie oben beschrieben ausgehandelt wird.

Weder SYNCING.NET Technologies noch andere Computer, die keine Mitglieder des jeweiligen Netzwerks sind, sind in der Lage die Daten zu entschlüsseln, da sie den geheimen Sitzungsschlüssel nicht kennen!

Der Grund für die Verwendung der Doppel-Verschlüsselung (AES + RSA) ist relativ einfach. Die symmetrische AES-Verschlüsselung und -Entschlüsselung ist schnell, sodass diese für die Sicherung des gesamten Datenverkehrs genutzt werden kann. Allerdings verwendet diese Verschlüsselungsmethode denselben (symmetrischen) Schlüssel, der beiden Kommunikationspartnern bekannt sein muss. Der RSA-Algorithmus basiert auf die Verwendung eines Schlüssel-Paares bestehend aus einem privaten und einem öffentlichen Schlüssel. Die 1024-Bit-RSA-Verschlüsselungsmethode gilt als sehr sicher, ist aber relativ langsam und erfordert eine schnelle CPU. SYNCING.NET verwendet sie deshalb nur für die Übertragung des AES-Sitzungsschlüssels sowie der eindeutigen Identifikationsnummer des jeweiligen Peers. Da diese Datenmenge sehr klein

ist - 32 Byte für den AES-Sitzungsschlüssel (32 Bytes = 256 Bits) plus einige Bytes für die Peer-ID - erfolgt die RSA-Verschlüsselung und -Entschlüsselung trotzdem sehr schnell.

Speicherung von Daten

Eine der Grundlagen unserer Datei- und Outlook-Synchronisation ist, dass keine Daten dauerhaft auf unseren Servern gespeichert werden und dass niemand Zugriff auf Ihre Daten erhält, sofern Sie ihn nicht bewusst dazu berechtigen.

Wenn die Option „*Store and Forward*“ aktiviert ist (Standard-Einstellung ab Version 2.0.3082), können Dateien und Outlook-Daten auch dann ausgetauscht werden, wenn die Computer einer Gruppe nicht gleichzeitig online sind. Die verschlüsselten Änderungsdaten des letzten online verbliebenen Teilnehmers werden dann komprimiert und zusätzlich mit dem individuellen 256-Bit-AES-Schlüssel kodiert temporär auf unserem Server zwischengespeichert. Nur der Zielcomputer kann die Dateien entschlüsseln. Sobald die Daten vom Zielcomputer heruntergeladen wurden, werden sie auf dem Server automatisch gelöscht. Falls die gespeicherten Daten nicht innerhalb von 14 Tagen heruntergeladen wurden, werden Sie automatisch von unseren Servern gelöscht.

Benutzersicherheit

Ihre Sync-Ordner bzw. Outlook-Gruppen sind grundsätzlich geschlossene Netzwerke und unterscheiden sich damit von den allgemein bekannten Filesharing-Anwendungen zum öffentlichen Austausch von z. B. Musikdateien. Niemand außer den Personen, die Sie explizit zu einem Sync-Ordner bzw. einer Outlook-Gruppe einladen, hat Zugriff auf Ihre Daten.

Zudem hat jeder Computer einen eindeutigen öffentlichen und privaten Schlüssel (1024-Bit-RSA-Verfahren) für die Nachrichten- und Benutzer-Authentifizierung. Die Übertragung von Daten ist erst zulässig, wenn ein Computer erfolgreich authentifiziert wurde. So können sowohl die Dateien, als auch die sonstige Kommunikation, nur von den von Ihnen eingeladenen Teilnehmern entschlüsselt werden, was Ihre Privatsphäre in einem hohen Maße schützt.

Datenschutz

Wir von SYNCING.NET respektieren und achten die Privatsphäre unserer Nutzer und tun alles, um Ihre persönlichen Daten zu schützen. Dazu haben wir eine verständliche Datenschutzerklärung entwickelt, um unsere Kunden zu schützen und jeden zu informieren, wie wir persönliche Daten verarbeiten. Unsere aktuelle Datenschutzerklärung finden Sie unter <http://www.syncing.net/de/meta/datenschutz.html>.