DATA.NOAH
BRINGT IHRE DATEN IN SICHERHEIT

White Paper

Sytemarchitektur DataNoah

Version 1.0

Datum 08.04.2018

DATA.**NOAH**, Nestroyplatz 1, 1020 Wien, Austria
Tel. +43 (0)1 311 31 88-0, Fax +43 (0)1 544 69 79-777, office@datanoah.at, www.datanoah.at

Impressum:

Data Noah GmbH
Nestroyplatz 1, A-1020 Wien
Tel. +43/1/311 31 88-0
Fax +43/1/544 69 79-777
http://www.datanoah.at

Disclaimer:

Dieses Dokument wurde nach bestem Wissen mit großer Sorgfalt zusammengestellt. Es dient im Wesentlichen dazu, Systemarchitektur, technische Installations- und Integrationsmöglichkeiten verschiedener Softwareprodukte von DataNoah zu erläutern. Abweichungen einzelner Funktionen von der jeweils verfügbaren Softwareversion, die von geringer oder kurzfristiger Bedeutung sind, sind möglich.

DataNoah macht keine Angaben zu einer bestimmten Eignung nachfolgender Informationen. Irrtümer und Fehler bleiben ausdrücklich vorbehalten und die Angaben erfolgen ohne Gewähr. Nachfolgende Informationen stellen nur Beschreibungen dar und enthalten keine Garantie der Beschaffenheit der Produkte. Die Informationen dienen als Hilfestellung und können auch ein Versuch sein, bei einer Aufgabenstellung zu helfen, selbst wenn das Produkt eigentlich nicht für diesen speziellen Zweck vorgesehen wurde.

Inhaltsverzeichnis

1 Allgemeines zu DataNoah Whitepapers

DataNoah Whitepapers enthalten Anleitungen bzw. Best Practice Szenarien zum Einsatz von DataNoah zur Datensicherung in unterschiedlichen IT-Umgebungen. Sie nehmen Bezug auf getestete bzw. praxiserprobte Installationen in gängigeren Umgebungen mit deren jeweiligen Besonderheiten.

Grundsätzlich ist der Inhalt des vorliegenden Dokuments als Informationsquelle bzw. Anleitung für IT-Techniker konzipiert, es werden also grundsätzliche Kenntnisse der aktuellen Microsoft oder anderer Betriebssysteme und IT-Infrastrukturkomponenten vorausgesetzt.

In diesem Dokument gegebenenfalls enthaltene Systemanpassungen müssen vor deren Durchführung mit der zuständigen IT-Administration abgeklärt werden bzw. erfolgen Änderungen grundsätzlich auf eigene Gefahr. Für eine Anpassung in einer zeitkritischen Produktivumgebung sollte unbedingt ein adäquater Testzeitraum mit einer Person, die entsprechende DataNoah Produktkenntnisse besitzt, eingeplant werden.

Gegebenenfalls enthält dieses Dokument Informationen bzw. Anleitungen zu Programmen von DataNoah, die Sie nicht lizenziert haben bzw. nicht anwenden.
Von DataNoah eingestellte bzw. nicht mehr gewartete Produkte werden in DataNoah Whitepapers nicht berücksichtigt.

2 Begriffsdefinitionen

- **Data Noah Software:**
  Dies sind zur Zeit die zwei Softwarelösungen DataNoah Manager und DataNoah Notebook, die als Backup Agents lokal am jeweiligen zu sichernden System installiert werden, die zu sichernden Daten ermitteln, verschlüsseln und an das DataNoah Rechenzentrum übermitteln.

- **DataNoah Rechenzentrum:**
  DataNoah Online Backup unterstützt die Datensicherung in zwei hochprofessionelle Rechenzentren in Wien und in Linz. Die Daten werden nicht außerhalb Österreichs gespeichert. In den DataNoah Rechenzentren werden die DataNoah Server betrieben.

- **DataNoah Server:**
  Der DataNoah Server speichert u.a. die Sicherungseinstellungen, überwacht Backup-Jobs, erstellt (Warn-)Meldungen und Berichte sowie Statistiken und überwacht die Kontingente sowie Health-Checks der gesamten Sytemkomponenten.

- **Verschlüsselung:**
  Die vom DataNoah-System zu sichernden Daten mit einem benutzerdefinierten Verschlüsselungskennwort verschlüsselt. Erst dann verlassen Daten die Kundensphäre und werden in das DataNoah Rechenzentrum oder auf ein lokales Sicherungsziel gesichert. Sämtliche von der DataNoah Software gesicherten Daten stellen für Dritte lediglich Datenmüll mit zufälligem Inhalt dar. Art und Weise bzw. Grad der Verschlüsselung kann vom Anwender selbst definiert werden. Erst mit der lokalen Eingabe des richtigen Verschlüsselungskennwortes können aus den gesicherten Daten im Rahmen des Wiederherstellungsvorgangs lesbare Daten hergestellt werden.

  Die Verschlüsselung der Daten ist per Design nicht abschaltbar. Selbst bei einem ausdrücklichen Wunsch des Anwenders besteht keine Möglichkeit, Daten durch DataNoah unverschlüsselt zu sichern.

- **Kundensphäre:**
  DataNoah richtet sich vor allem an Anwender mit kritischen Daten. Hier ist die Sensibilität der Frage wo sich Anwenderdaten befinden bzw. wo spezifische Datensicherungsfunktionen ablaufen besonders hoch. Um transparent zu machen, was wo mit Daten des Anwenders passiert, beschreibt die Kundensphäre bei DataNoah aus einer Security-Sicht heraus jenen Bereich, der komplett der Kontrolle des Anwenders unterliegt. Dies sind z.B. all jene Geräte (Server, PCs, Notebooks), die der physischen Kontrolle des Anwenders unterstehen bzw. in denen Softwarekomponenten laufen, die der softwaretechnischen (Installation, Betrieb) Kontrolle des Anwenders zuzuordnen sind.

3 DataNoah Systemarchitektur

Das OnlineBackup System besteht architektonisch grundlegend aus zwei Komponenten, der OnlineBackup Sicherungssoftware und dem OnlineBackup Server, die untereinander in Interaktion treten und sich die Aufgaben der gesamtheitlichen Datensicherungslösung teilen.

Das architektonische Konzept sieht eine möglichst optimale Kombination von sicherheitstechnischen und funktionalen Aspekten vor.

So findet die Komprimierung und Verschlüsselung der zu sichernden Daten ausschließlich kundenseitig statt, die Hinterlegung der Verschlüsselungsschlüssel und der Kennwörter für den Zugang zu Sicherungsquellen befinden sich ebenso zu jeder Zeit verschlüsselt ausschließlich auf Kundenseite und werden niemals an den OnlineBackup Server übertragen.

Um eine praxisnahe Funktionsvielfalt und Kontrollmechanismen, die ein nachhaltig hohes Qualitätsniveau des Dienstes gewährleisten, zu erreichen, werden Einstellungen (immer ohne Kennwörter) aller Sicherungssätze inklusive deren Ausführungszeitpläne am OnlineBackup Server hinterlegt. Die Hinterlegung erfolgt dabei in strenger Assoziation zum Kundenaccount, der am OnlineBackup Server die höchste Hierarchieebene darstellt.

Auf diese Weise kann der OnlineBackup Server Kontrollmechanismen, wie das Versenden von Benachrichtigen aller Art vornehmen, auch wenn das Kundensystem z.B. gar nicht in Betrieb ist oder vom Netzwerk bzw. Internet getrennt wurde.

Hintergrundaktivitäten wie die periodischen CRC-Prüfungen über alle gesicherten Datenbestände, ständige Bereinigungsarbeiten alter Archivstände gemäß definierter Richtlinien und eine laufende Kontingentüberwachung gewährleisten zu jeder Zeit den nachhaltigen Wert des Datensicherungsservices und finden auf Seite des OnlineBackup Server statt.

Im Folgenden werden wesentliche Basisfunktionen der beiden architektonischen Hauptkomponenten unserer OnlineBackup Lösung gelistet, um die Differenzierung der Aufgabenteilung auszudrücken.

3.1 Basisaufgaben der DataNoah Software (nicht abschließend)

- Assoziation mit einem OnlineBackup Kundenaccount
- Anlage und Detaildefinition von Sicherungssätzen
- Automatische, zeitgesteuerte Sicherung pro Sicherungssatz gemäß definierten Zeitplänen
- Abgleich der Versionsstände aller gesicherten Daten mit dem OnlineBackup Server
- Manuelle Datensicherung pro Sicherungssatz aus dem Programm angestoßen
- Initialsicherung auf externe Datenträger
- Wiederherstellung von externen Datenträgern
- Sicherung /Abgleich der Einstellungen pro Sicherungssatz auf den OnlineBackup Server
- Abruf der serverseitigen Informationen zum Status der Sicherungssätze und Kontingente

3.2 Basisaufgaben des DataNoah Servers (nicht abschließend)

- Anlage eines OnlineBackup Kundenaccounts
- Authentifizierung der OnlineBackupsoftware bei jedem Login/Sicherungsvorgang
- Empfang der Einstellungen pro Sicherungssatz und deren verschlüsselte Ablage
- Empfang der verschlüsselten Sicherungsdaten und deren Ablage
- Abgleich der Versionsstände aller gesicherten Daten mit dem OnlineBackup Server
- Abruf definierter Stände zur Wiederherstellung über die OnlineBackup Software
- Abruf definierter Stände zur Wiederherstellung über das gekapselte Java-Applet
- Abruf der gesamten Stände pro Kundenaccount zum Transfer auf externe Datenträger
- Laufende Kontingentüberwachung pro Kundenaccount
- Laufende Archivbereinigungstätigkeiten entsprechend Richtlinien pro Sicherungssatz
- Überwachung sämtlicher Sicherungsvorgänge gemäß deren Zeitpläne auf deren Status
- Periodische CRC-Prüfungen über alle Bestände pro Sicherungssatz
- Kundenportal zur Einsicht allerBerichte und Kontingente sowie zur Anpassung div. Einstellungen Ständige Health-Checks aller Systemkomponenten und technische Hintergrundaufgaben
- Meldungs- und Berichtswesen zur Generierung aller Reports und Versand aller Benachrichtigungen

4 Schritte der Datensicherung

Initiierung des Sicherungsvorgangs per Zeitplan oder manuell innerhalb der DataNoah Software.

↓

Abruf/Abgleich der Versionsstände der letzten Sicherung des Sicherungssatzes von/mit dem DataNoah Server.

↓

Auslesen der Sicherungsquelle, Erfassen der Dateiversionen, Erstellen einer Versionsliste, Abgleich der Versionsliste mit jener der Letztsicherung, Erstellen der Liste der zu sichernden Dateien.

↓

Start der Dateiübertragung geänderter Daten gemäß der erstellten Liste und Prüfung größerer Dateien gemäß definiertem Schwellenwert auf Datei-Delta-Bildung in den ebenfalls definierten temporären Pfad. Falls eine Delta-Bildung zutreffend ist, werden gemäß der letztgültigen Sicherung die Änderungen innerhalb der Datei auf Blocklevel errechnet, auf den definierten prozentuellen Schwellenwert hin überprüft und falls wiederum zutreffend, die geänderten Blöcke aus der Datei geschrieben.

↓

Nach Beendigung des Schreibens einer Dateigruppe in den temporären Pfad werden diese komprimiert, mit dem Verschlüsselungsschlüssel für diesen Sicherungssatz verschlüsselt und an den DataNoah Server hochgeladen, während die Dateiübertragung weiterer geänderter Dateien in den temporären Pfad fortgesetzt wird.

↓

Nach Beendigung der Datensicherung werden der Sicherungsstatus, das Protokoll und die Versionsliste an den DataNoah Server gesendet. Der Vorgang ist für die DataNoah Software damit abgeschlossen.

↓

Nun verarbeitet der DataNoah Server die empfangenen Statusdaten, aktualisiert damit den entsprechenden Sicherungssatz und übergibt den Sicherungsstatus für die entsprechende Benachrichtigung an das interne Melde- und Berichtswesen.

5 Datensicherung auf einen externen Datenträger

Die OnlineBackup Software bietet für drei verschiedene Vorgänge die Möglichkeit, Daten nicht (nur) auf den entfernten OnlineBackup Server zu sichern, sondern auf einen beliebigen (auch externen) Datenträger, der von der OnlineBackup Software aus erreichbar ist, zu übertragen.

Exakt wie auch beim Sicherungsvorgang auf den OnlineBackup Server werden die zu sichernden Daten komprimiert und mittels des Verschlüsselungsschlüssels des jeweiligen Sicherungssatzes 256-bit verschlüsselt. Nun werden die verschlüsselten Daten allerdings nicht über den 128-bit verschlüsselten SSL-Kanal zum OnlineBackup Server übertragen, sondern über das Dateisystem oder über das lokale Netzwerk zum Zieldatenträger gesendet.

In den folgenden drei Szenarien ist oben Erwähntes relevant:

5.1 Initialsicherung

Wenn eine OnlineBackup Software neu eingerichtet wird und einmalig große Datenmengen auf den OnlineBackup Server zu transferieren sind, welche für die bestehende Internetverbindung nicht oder nur schwer in überschaubarer Zeit übertragbar sind, besteht die Möglichkeit, diese Daten temporär auf einen externen Datenträger zu sichern, diesen beispielsweise per Post (Daten sind verschlüsselt/absolut unlesbar) an uns zu senden und wir nehmen das Einspielen auf den OnlineBackup Server vor (wird von uns konventionell an den richtigen Platz kopiert).

Ab diesem Zeitpunkt erkennen Software und Server den auf diese Weise übertragenen Datenbestand an, als wäre er konventionell über das Internet übertragen worden und der Sicherungslauf kann gemäß dem eingestellten Zeitplan uneingeschränkt erfolgen.

5.2 Zusatzsicherung

Vorwiegend für die Notwendigkeit eines raschen Desaster Recoverys, aber auch aus anderen Gründen, kann es sinnvoll sein, die mit der OnlineBackup Software gesicherten Daten nicht nur an den entfernten OnlineBackup Server zu übertragen, sondern parallel dazu auch eine lokale Zusatzsicherung auf einem Serverlaufwerk/NAS-Gerät oder einer externen Festplatte zu betreiben. Die zusätzliche Sicherung wird im Sicherungssatz definiert und läuft gemäß dem eingestellten Sicherungszeitplan völlig parallel.

Bei raschem Wiederherstellungsbedarf großer Datenmengen besteht der Vorteil einer sehr raschen Wiederherstellbarkeit der gesicherten Daten, die über die OnlineBackup Software von dem Netzlaufwerk bzw. externen Datenträger direkt wiederherstellt werden können.

5.3 Zusatzsicherung

Sind nach einem Totalschaden vor Ort sämtliche Daten vernichtet worden und besteht im Zuge des Neuaufbaus bzw. eines interimistischen Notbetriebs rasch Bedarf an den gesicherten Daten, können die verschlüsselten Daten am OnlineBackup Server auch von uns auf einen bereitgestellten externen Datenträger kopiert und an den Zielort transportiert werden. In diesem Fall muss die OnlineBackup Software am Zielort auf einem Rechner neu installiert werden und der Verschlüsselungsschlüssel unbedingt bekannt sein, da die auf dem externen Datenträger bereitgestellten Daten nur damit wiederherstellt werden können.

6 128-bit-SSL Kommunikation

Sämtliche Kommunikation zwischen der lokalen OnlineBackup Software und dem OnlineBackup Server wird über einen 128-bit verschlüsselten SSL (Secure Socket Layer) Kanal geführt. Das gilt für Authentifizierungs- und Steuerungsparameter als auch für die bereits zuvor komprimierten und verschlüsselten Sicherungsdaten.

Obwohl sich die Daten also über das öffentliche Netzwerk bewegen, kann niemand – außer die Quelle und das Ziel – Kenntnis über den Sinn und Inhalt der Pakete erhalten. Darüber hinaus hat ausschließlich die Quelle (OnlineBackup Software) Kenntnis über die tatsächlichen, zur Sicherung bestimmten Daten. Die Gegenstelle (OnlineBackup Server) hat hingegen nur Kenntnis über die bereits verschlüsselten Daten.

7 Verschlüsselung

Alle zu sichernden Dateien werden von der DataNoah Software zuerst komprimiert und mit dem benutzerdefinierten Verschlüsselungspasswort verschlüsselt, bevor sie an den DataNoah Server oder ein lokales Sicherungsziel versendet werden.

Sämtliche, von der DataNoah Software gesicherten Dateien sind für Dritte ausschließlich Datenmüll mit verschlüsseltem, nicht lesbarem Inhalt. Eine Wiederherstellung der Daten ist allein möglich, sofern man in Kenntnis des passenden Verschlüsselungspassworts ist, denn nur damit und mit Hilfe der DataNoah Software als Werkzeug ist man in der Lage, im Rahmen eines Wiederherstellungsvorgangs lesbare Daten aus den gesicherten Beständen zu erstellen.

7.1 Definition des Verschlüsselungsschlüssels pro Sicherungssatz

Der Verschlüsselungsschlüssel ist – wie bereits erwähnt – eine der zentralsten Komponenten in der Architektur und im Prozess des DataNoah Systems. Keine Daten verlassen das jeweilige lokale System, ohne zuvor verschlüsselt worden zu sein. Sämtliche gesicherten Bestände sind und bleiben ohne diesen jeweiligen passenden Schlüssel ausschließlich Datenmüll.

Entsprechend wichtig sind vorbereitende Überlegungen zur Wahl des bzw. der geeigneten Schlüssel und zur sicheren Hinterlegung derselben für den Notfall.

Zugunsten einer möglichst flexiblen und benutzerdefinierbaren Sicherheitsstufe bieten wir die Möglichkeit der Wahl eines jeweils eigenständigen Schlüssels pro Sicherungssatz innerhalb der DataNoah Software an. Diese Möglichkeit kann die höchsten Sicherheitsbedürfnisse erfüllen, da man dann zu Beispiel auch einen Datenbestand in mehrere Sicherungssätze mit jeweils unterschiedlichen Schlüsseln unterteilen könnte und somit die Daten in Ihrer Wiederherstellbarkeit voneinander trennen kann. Diese Option bietet sich an, wenn innerhalb einer Organisation Datenbereiche mit unterschiedlichen Zugangsberechtigungen existieren.

So könnten z.B. unterschiedliche Backup Sets erstellt werden, die einerseits von hausinternen IT-Administratoren verwaltet werden können und solche Backup-Sets mit besonders sensiblen Daten, die deren Zugriff und Wiederherstellbarkeit allein dem Management vorbehalten sein soll.

Die Vielfalt der Einstellungsmöglichkeiten für die Verschlüsselung pro Backup Set bringt allerdings auch die erweiterte Gefahr verlorengegangener Schlüssel mit sich. Aus diesem Grund schlägt die DataNoah Software beim Assistenten zu einem neuen Sicherungssatz beim Thema Verschlüsselung die Option “Standard“ vor, die die Verwendung des gegenwärtigen Benutzerkennworts des aktuellen Benutzers der OnlineBackup Software als Verschlüsselungsschlüssel ermöglicht.

Wichtige Aufklärung:

Die im Rahmen von DataNoah von Ihnen gesicherten Daten werden auf unseren Servern in hochverschlüsselter Form gespeichert. Die Daten können nach derzeitigem Stand der Technik nicht ohne das von Ihnen gewählte Sicherungskennwort entschlüsselt werden. Bei Verlust Ihres Sicherungskennwortes besteht – auch für DataNoah – keine Möglichkeit Ihre Daten in lesbarer Form wiederherzustellen. Sie selbst sind für die sichere Aufbewahrung des von Ihnen gewählten Kennwortes zuständig, wir empfehlen die Verwahrung in einem Bankschließfach oder die Hinterlegung bei Ihrem Rechtsanwalt/Notar.

ES BESTEHT – AUCH FÜR DATANOAH – KEINE TECHNISCHE MÖGLICHKEIT, DIESES KENNWORT WIEDERHERZUSTELLEN.

7.2 Schutz des Verschlüsselungsschlüssels

Die Verschlüsselungsschlüssel, die benutzt werden, um die zu sichernden Dateien zu verschlüsseln, sind ausschließlich am lokalen Computer hinterlegt, auf dem die jeweilige DataNoah Software installiert ist und ausgeführt wird.

Dennoch sind die Schlüssel auch direkt am lokalen Computer in keiner lesbaren Form abgelegt sondern befinden sich – chiffriert – in der konkreten Datei config.sys.

Technische Details:

Speicherort der Datei config.sys, welche die chiffrierten Verschlüsselungsschlüssel aller Sicherungssätze, die mittels der lokalen OnlineBackup Software konfiguriert sind, enthält:

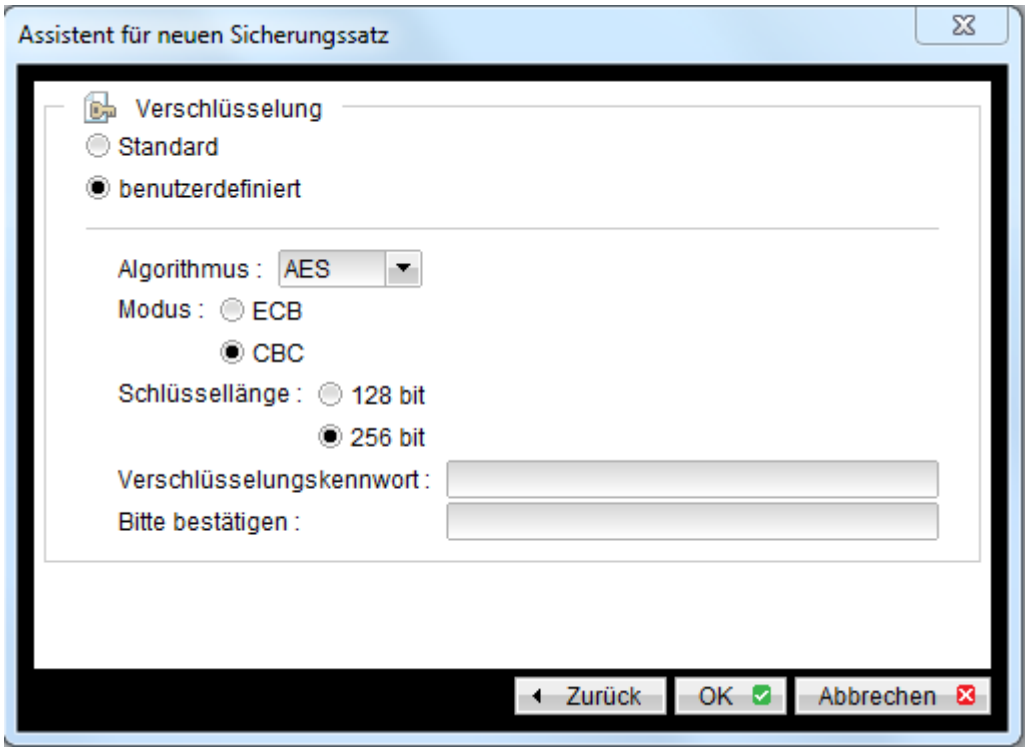
Windows-Systeme:	%USERPROFILE%\.obm\config\config.sys
Linux-Systeme:	~/.obm/config/config.sys
Mac OS X:	~/.obm/config/config.sys

Wenn die DataNoah Software die Datei config.sys nicht finden kann (z.B. durch versehentliches Löschen, Einloggen mit einem anderen Benutzer, Einloggen auf einer neu installierten DataNoah Software auf einem neuen Gerät mit einem bestehenden Benutzeraccount, etc.), erfordert die Software mittels Aufforderungsfenster die erneute Eingabe der Verschlüsselungsschlüssel für die unter dem eingeloggten Benutzeraccount existierenden Sicherungssätze und speichert diese nach erfolgreicher Eingabe wieder – natürlich proprietär chiffriert – in der lokalen Datei config.sys.

7.3 Verschlüsselungsalgorithmus

Der aktuell standardmäßig von unserem OnlineBackup System benutzte Algorithmus zur Verschlüsselung aller zu sichernden Dateien ist Advanced Encryption Standard (AES) mit 256-bit Blockverschlüsselung (Betriebsmodus CBC). Dieser Verschlüsselungsstandard wurde von einer größeren Sammlung, die ursprünglich als Rijndael veröffentlicht wurde, adaptiert. AES ist die erste öffentlich verfügbare Verschlüsselung, die von mehreren Geheimdiensten weltweit für die Chiffrierung streng geheimer Informationen zertifiziert wurde.

Benutzt man bei der Erstellung eines neuen Sicherungssatzes innerhalb der OnlineBackup Software beim Thema Verschlüsselung nicht die Standardoption, bei der das aktuelle Kennwort des Benutzeraccounts als Verschlüsselungsschlüssel dient (hier erfolgt standardmäßig 256-bit AES Verschlüsselung mit Betriebsmodus CBC), erhält man zusätzlich zur Wahl des zu vergebenden Verschlüsselungsschlüssels drei Optionen zur Wahl des Verschlüsselungsstandards (AES, Twofish, DESede), zwei Optionen zur Wahl des Betriebsmodus (ECB, CBC) und weitere zwei Optionen zur Wahl der Schlüssellänge (128-bit, 256-bit).



Diese Wahlmöglichkeiten der Verschlüsselung dienen vorwiegend dem Bedarfsfall spezieller, eventuell vorliegender Compliance-Anforderungen, außerdem verhalten sich einzelne kryptographische Kombinationen in sehr spezifischen Anwendungsfällen performanter.

Wenn kein spezieller Grund existiert, empfehlen wir ausdrücklich die Verwendung des Verschlüsselungsstandards AES mit 256-bit Blockverschlüsselung im Betriebsmodus CBC.

8 DataNoah User Account

Für den Betrieb jeder Installation der OnlineBackup Software ist ein aus Benutzername und Kennwort bestehender User Account erforderlich. Das Kennwort kann jederzeit über die OnlineBackup Software geändert werden.
Der User Account dient der Authentifizierung an der OnlineBackup Software und am OnlineBackup Server der Verwaltung aller zugehörigen Eigenschaften, Einstellungen, Sicherungssatzeigenschaften und der verschlüsselten, gesicherten Daten- und Archivbestände.

Benutzername und Kennwort des User Accounts wird hochverschlüsselt am lokalen System, auf dem die OnlineBackup Software installiert ist, sowie am OnlineBackup Serversystem abgelegt.

9 Daten zur Authentifizierung an Server-/Netzwerkressourcen

Dieser Punkt ist Bestandteil von -> Sicherung der Einstellungen auf den OnlineBackup Server

10 Wiederherstellung verschlüsselter Daten

Durch das Konzept, der Archivierung ausschließlich verschlüsselter Daten im DataNoah Rechenzentrum reicht es zur Wiederherstellung von (lokal gelöschten) Daten nicht allein aus, Daten aus dem Rechenzentrum auf die lokalen IT-Systeme zu kopieren. Durch die oben beschriebene strenge Trennung zwischen Kundensphäre und DataNoah Rechenzentrum müssen die archivierten Daten nach dem Transfer aus dem DataNoah Rechenzentrum wieder entschlüsselt werden.

In der Praxis erfolgt dieser Schritt auf zwei mögliche Arten der Wiederherstellung:

- DataNoah Software
- Java-Applet, das lokal am Client des Anwenders läuft

10.1 DataNoah Software

Eine Wiederherstellung von Daten am lokalen System ist sehr einfach möglich über die DataNoah Software. Mit der Auswahl der Daten, die wiederhergestellt werden sollen, setzt DataNoah den Übertragungsprozess der verschlüsselten Daten aus dem DataNoah Rechenzentrum in Gang. Nach der Übertragung dieser verschlüsselten Daten auf das lokale System werden diese mit Hilfe des in der lokalen Data Noah Software hinterlegten Verschlüsselungskennwortes wieder entschlüsselt. Sollte kein Verschlüsselungskennwort hinterlegt sein, so wird zur Eingabe des passenden Kennwortes aufgefordert.

10.2 Wiederherstellung durch das Kundenportal

Es besteht für den Fall des dringenden Bedarfs gesicherter Daten die Möglichkeit, eine Wiederherstellung der gesicherten Daten auch ohne den Einsatz der OnlineBackup Software am lokalen System vorzunehmen.

Dazu startet man nach erfolgreichem Login mit den Daten des entsprechenden OnlineBackup User Accounts über den entsprechenden Link das Java-Wiederherstellungsapplet. Es enthält begrenzte gekapselte Funktionen zur Wiederherstellung von Daten aus Sicherungssätzen. Das Java-Applet läuft nicht am DataNoah Server sondern im lokalen Browser des Anwenders.

Um zu den wiederhergestellten Daten zu gelangen, ist selbstverständlich die Eingabe des Verschlüsselungsschlüssels erforderlich, selbst wenn es um eine Verschlüsselung mit dem Kennwort des User Accounts handelt.

Der Verschlüsselungsschlüssel wird während der Laufzeit des gekapselten Java Applets ausschließlich im Speicher gehalten und niemals auf das ausführende System geschrieben.

10.3 Optionale IP-Einschränkung für Wiederherstellung von gesicherten Daten

Als weiteres Sicherheitsmerkmal ist es beim DataNoah System auf jederzeitigen Wunsch möglich, die Wiederherstellung von Daten vom DataNoah Server auf IP-Adressen zu beschränken.

Wird bei aktivierter Einschränkung versucht, Daten vom DataNoah Server wiederherzustellen und ist die IP-Adresse der Quelle dieser Wiederherstellungsanforderung nicht in der entsprechenden Adressliste definiert, wird der Zugriff verweigert, selbst wenn Benutzername und Kennwort des Accounts sowie der Verschlüsselungsschlüssel bekannt sind.

Diese Beschränkung gilt sowohl bei Wiederherstellungsversuchen aus der DataNoah Software als auch mittels dem Wiederherstellungsapplet, das aus dem DataNoah Kundenportal angestoßen werden kann.

In der Praxis erfolgt dieser Schritt auf zwei mögliche Arten der Wiederherstellung:

- DataNoah Software
- Java-Applet, das lokal am Client des Anwenders läuft

10.4 DataNoah Software

Eine Wiederherstellung von Daten am lokalen System ist sehr einfach möglich über die DataNoah Software. Mit der Auswahl der Daten, die wiederhergestellt werden sollen, setzt DataNoah den Übertragungsprozess der verschlüsselten Daten aus dem DataNoah Rechenzentrum in Gang. Nach der Übertragung dieser verschlüsselten Daten auf das lokale System werden diese mit Hilfe des in der lokalen Data Noah Software hinterlegten Verschlüsselungskennwortes wieder entschlüsselt. Sollte kein Verschlüsselungskennwort hinterlegt sein, so wird zur Eingabe des passenden Kennwortes aufgefordert.

10.5 Wiederherstellung durch das Kundenportal

Es besteht für den Fall des dringenden Bedarfs gesicherter Daten die Möglichkeit, eine Wiederherstellung der gesicherten Daten auch ohne den Einsatz der OnlineBackup Software am lokalen System vorzunehmen.

Dazu startet man nach erfolgreichem Login mit den Daten des entsprechenden OnlineBackup User Accounts über den entsprechenden Link das Java-Wiederherstellungsapplet. Es enthält begrenzte gekapselte Funktionen zur Wiederherstellung von Daten aus Sicherungssätzen. Das Java-Applet läuft nicht am DataNoah Server sondern im lokalen Browser des Anwenders.

Um zu den wiederhergestellten Daten zu gelangen, ist selbstverständlich die Eingabe des Verschlüsselungsschlüssels erforderlich, selbst wenn es um eine Verschlüsselung mit dem Kennwort des User Accounts handelt.

Der Verschlüsselungsschlüssel wird während der Laufzeit des gekapselten Java Applets ausschließlich im Speicher gehalten und niemals auf das ausführende System geschrieben.

10.6 Optionale IP-Einschränkung für Wiederherstellung von gesicherten Daten

Als weiteres Sicherheitsmerkmal ist es beim DataNoah System auf jederzeitigen Wunsch möglich, die Wiederherstellung von Daten vom DataNoah Server auf IP-Adressen zu beschränken.

Wird bei aktivierter Einschränkung versucht, Daten vom DataNoah Server wiederherzustellen und ist die IP-Adresse der Quelle dieser Wiederherstellungsanforderung nicht in der entsprechenden Adressliste definiert, wird der Zugriff verweigert, selbst wenn Benutzername und Kennwort des Accounts sowie der Verschlüsselungsschlüssel bekannt sind.

Diese Beschränkung gilt sowohl bei Wiederherstellungsversuchen aus der DataNoah Software als auch mittels dem Wiederherstellungsapplet, das aus dem DataNoah Kundenportal angestoßen werden kann.

11 Obligatorische E-Mail-Benachrichtigungen

Benachrichtigungen per E-Mail an eine oder mehrere im User Account hinterlegte E-Mail-Adressen sind bei unserem OnlineBackup System obligatorisch.

Der hinterlegte Benutzer wird dabei über erfolgreiche, mit Warnungen erfolgte, fehlgeschlagene und nicht nach Plan stattgefundene Sicherungsvorgänge sowie systemseitige Meldungen wie u.a. entdeckte Fehler im gesicherten Datenbestand im Rahmen der regelmäßigen CRC-Prüfungen und sich erschöpfende Sicherungskontingente informiert.

Die E-Mails werden dabei vom OnlineBackup Server, entweder aufgrund von Informationsmeldungen der OnlineBackup Software an den OnlineBackup Server oder aufgrund eigener auslösender Prozesse des OnlineBackup Servers, versendet.

In vielen Firmen und Organisationen ist genau dies für besonders sensible Daten nicht gewünscht. So soll z.B. die hausinterne IT-Administration zwar dafür verantwortlich sein, alle unternehmenskritischen Daten verlässlich zu sichern und ggf. wiederherzustellen. Möglicherweise sollen aber bestimmte Datenbereiche, z.B. die interne Lohnverrechnung, auf die nur wenige Personen im Unternehmen Zugriff haben, auch während des Sicherungs- und Wiederherstellungsprozesses im Rahmen einer Backup-Strategie nur von diesen wenigen Personen wiederhergestellt werden können.

12 Sicherung der Einstellungen auf den OnlineBackup Server

Nachdem man sich nach der erstmaligen Installation der OnlineBackupsoftware mit von uns zur Verfügung gestellten Accountdaten anmeldet, die initialen Sicherungssätze erstellt und diese Einstellungen anschließend über den entsprechenden Button sichert, werden die getroffenen Einstellungen am lokalen System verschlüsselt abgelegt und im Anschluss über die verschlüsselte SSL-Verbindung zum OnlineBackup Server an diesen übertragen und streng mit dem User Account assoziiert wiederum verschlüsselt abgelegt.

Wird in weiterer Folge ein neuer Sicherungssatz angelegt oder ein bestehender Satz geändert, werden diese Einstellungen am lokalen System aktualisiert und danach wieder an den OnlineBackup Server zurückgeschrieben – was wiederum über die verschlüsselte SSL-Verbindung erfolgt.

Die Einstellungen bleiben dabei selbstverständlich bei jeder Aktualisierung verschlüsselt abgelegt.

Werden lokale Zugangsdaten zu Sicherungsquellen (administrativer Benutzeraccount z.B. für die Dateisicherung, die SQL-Datenbanksicherung, die Exchange Informationstore Sicherung oder die Exchange Mail-Level-Sicherung im Sicherungssatz innerhalb der OnlineBackup Software angegeben, so wird der der entsprechende Benutzername zu den allgemeinen Einstellungen des jeweiligen Sicherungssatzes gespeichert und somit – wie bereits oben beschrieben – auf den OnlineBackup Server übertragen, das entsprechende Kennwort jedoch ausschließlich lokal getrennt abgelegt und verschlüsselt – es erfolgt also kein Zurückschreiben auf den OnlineBackup Server.

Das Zurückschreiben der Einstellungen von der OnlineBackup Software auf den OnlineBackup Server erlaubt elementare Funktionen wie z.B. die Benachrichtigung bei nicht stattgefundener Sicherung, die somit auch dann erfolgen kann, wenn die lokale OnlineBackup Software nicht läuft, weil der Server z.B. abgeschalten ist oder sich sonst in keinem reaktionsfähigem Zustand befindet bzw. über längere Zeit keine Internetverbindung vom lokalen Server aufgebaut werden kann.

Ebenso kann eine Wiederherstellung der Einstellungen vom OnlineBackup Server auf die OnlineBackup Software erfolgen, wenn z.B. der Server neu aufgesetzt werden musste und so eine Neuinstallation der Software unter Verwendung derselben User Account Daten erforderlich ist.

Voraussetzung hierzu ist allerdings ein gleichlautender Servername, da die bestehenden Sicherungssätze sonst nicht automatisch wiederhergestellt werden.

Sollten innerhalb des jeweiligen Sicherungssatzes Benutzerdaten für den Zugriff auf Sicherungsquellen angegeben worden sein, muss im Fall der Wiederherstellung der Einstellungen vom OnlineBackup Server das jeweilige Kennwort neu eingegeben werden, da es - wie oben beschrieben –niemals auf den OnlineBackup Server übertragen wird.