DATA.NOAH
BRINGT IHRE DATEN IN SICHERHEIT

White Paper

Security 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 Einführung: Sicherheitsarchitektur DataNoah

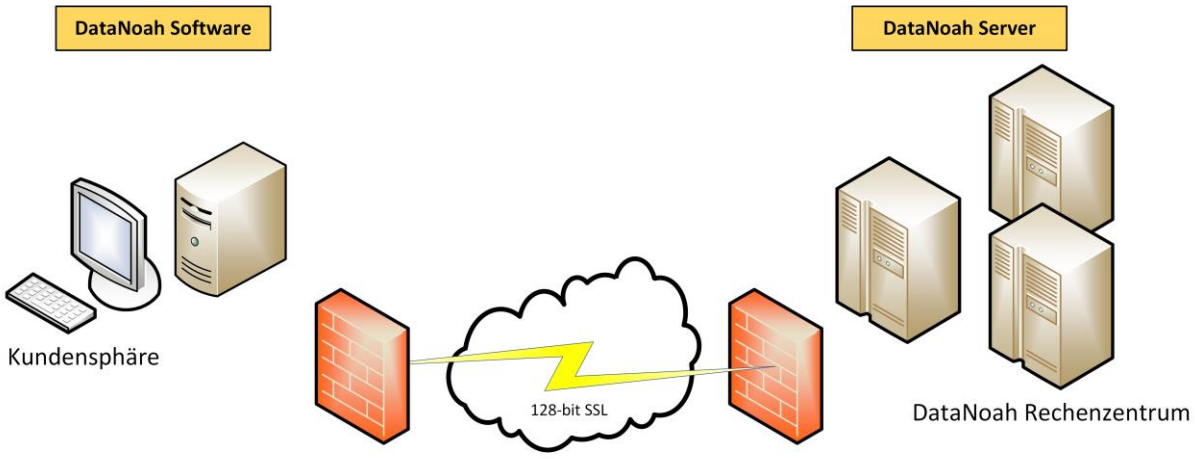
Die DataNoah Online-Datensicherung wurde entwickelt, um folgende Bedürfnisse optimal abzudecken:

- Unternehmenskritische Daten werden außerhalb der Betriebsräumlichkeiten sicher archiviert,
- Sensible Daten (Kundendaten, Mandantendaten, Geschäftsgeheimnisse) werden sofort und bereits im Kontrollbereich des Anwenders hoch verschlüsselt,
- Verschlüsselte Daten werden in einem professionellen Rechenzentrum gesichert,
- Wiederherstellung von archivierten Daten ist jederzeit möglich.
- Vollautomatische Überwachung der Datensicherung durch Zwei-Komponenten-Strategie (Anstoß der Sicherung durch DataNoah Client, gleichzeitige Überwachung der Sicherung durch DataNoah Rechenzentrum),
- Erfüllung von Sorgfaltspflichten, die sich auf der Basis gesetzlicher (z.B. UGB), vertraglicher, standesrechtlicher oder anderer Verpflichtungen ergeben.

Weil das Bedürfnis nach externer professioneller Datenspeicherung gerade in Branchen mit hoher Datansensibilität gegeben ist, wurde Wert auf eine sehr klare Sicherheitsarchitektur gelegt. Die DataNoah Online Datensicherung basiert auf zwei Grundprinzipien:

- Daten des Anwenders verlassen zu keinem Zeitpunkt unverschlüsselt die Kontrollsphäre des Anwenders und
- die Verschlüsselung der Daten erfolgt durch Verschlüsselungskennwort, das allein dem Anwender bekannt ist.

Wie diese Prinzipien im DataNoah-System umgesetzt sind, wird in diesem White Paper beschrieben.

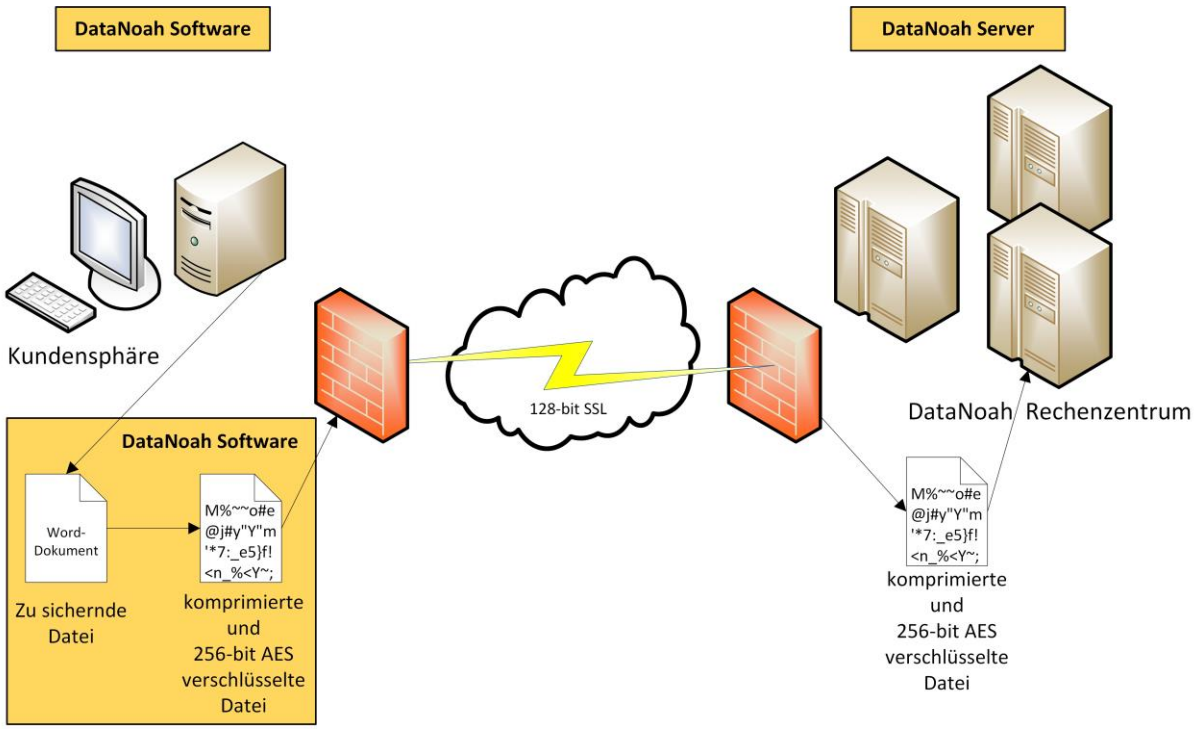


Sämtliche Kommunikation findet über eine 128-bit SSL Verbindung
statt – auch die bereits zuvor verschlüsselten Sicherungsdaten

4 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.



4.1 Definition des Verschlüsselungsschlüssels pro Sicherungssatz

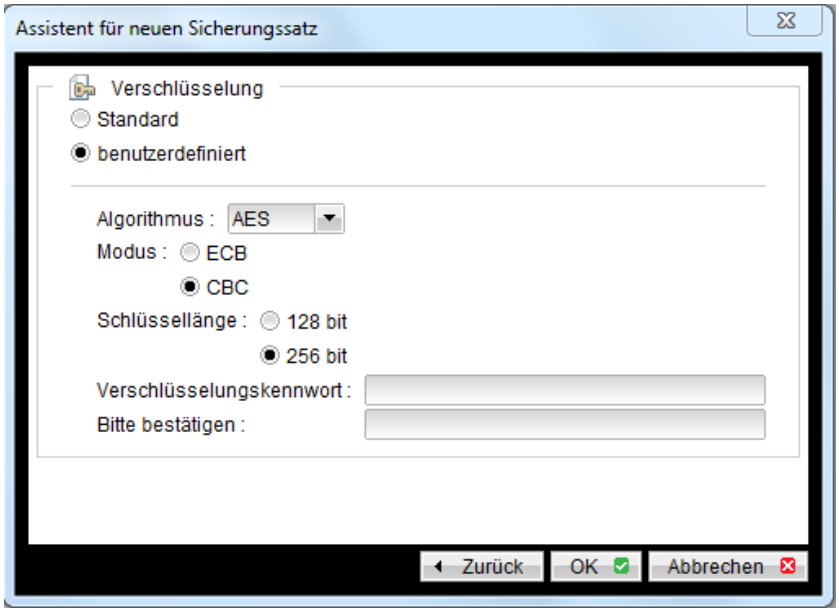
Der Verschlüsselungsschlüssel ist – wie bereits erwähnt – eine der zentralsten Komponenten in der Architektur und im Prozess des DataNoah Systems. Keine Daten verlassen das jeweilige lokale System, ohne zuvor verschlüsselt worden zu sein. Sämtliche gesicherten Bestände sind und bleiben ohne diesen jeweiligen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

4.2 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 – verschlüsselt – 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:

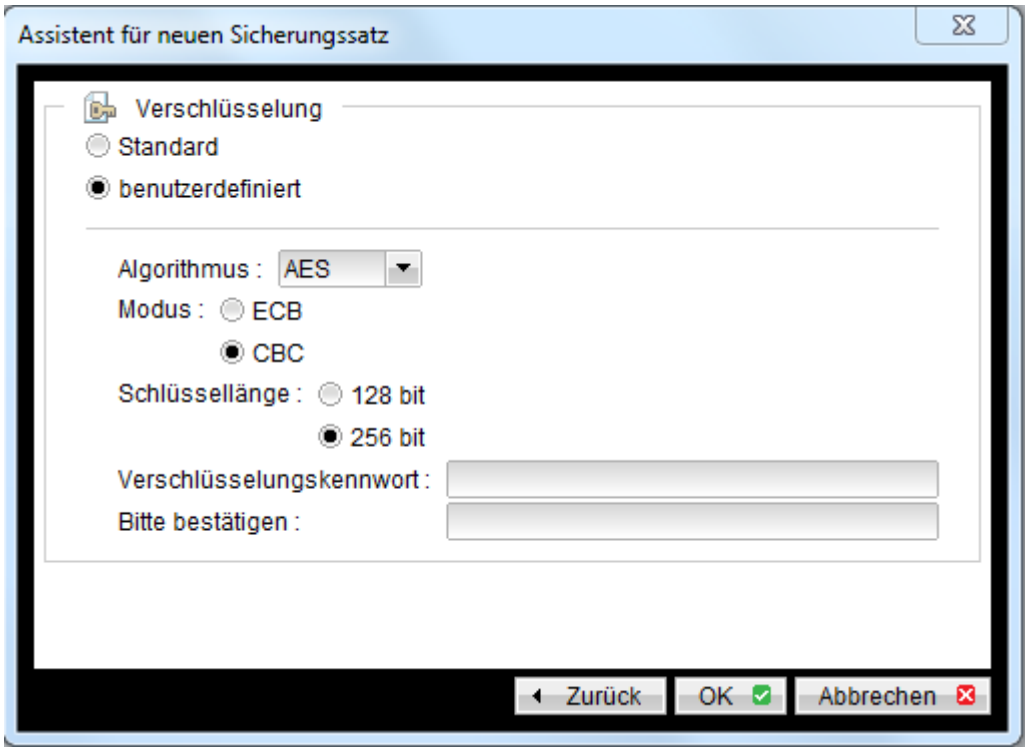
Windows-Systeme:	%USERPROFILE%\.obm\config\config.sys
Linux-Systeme:	~/.obm/config/config.sys
Mac OS X:	~/.obm/config/config.sys

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 verschlüsselt – in der lokalen Datei config.sys.

4.3 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.

4.4 Rechenbeispiel zur Sicherheit der 256-bit Verschlüsselung

Eine 256-bit Schlüsselgröße besitzt 2^{256} oder etwa 1,16 x 10^{77} mögliche Kombinationen.

Selbst der aktuell weltbeste Supercomputer Tianhe-2, welcher 16.000 Rechenknoten mit 3,2 Millionen Kernen besitzt (u.a. 32.000 × Intel Xeon E5-2692 (12-Core-Prozessor, „Ivy Bridge“, 2,2 GHz, 211 GFLOPS) und 48.000 × Intel Xeon Phi 31S1P (57-Core-Prozessor, 1,1 GHz)) und von der chinesischen Nationaluniversität für Wehrtechnologie Mitte 2013 entwickelt und fertiggestellt wurde, benötigt theoretische 1,086 x 10^{53} Jahre, um alle Kombinationen zu testen. (siehe unten)

Dieser Supercomputer bietet eine gesamte Rechenkapazität von 33,86 Petaflops.

Wir gehen davon aus, dass der Rechner in einer Computer Operation eine mögliche Kombination testen kann (was schneller als möglich ist).

Wird Brute Force Attack (alle Kombinationen prüfen) gegen diesen Verschlüsselungsalgorithmus verwendet, benötigt der Supercomputer bei oben erwähnter idealistischer Annahme

$$\frac{1{,}16 \text{ x } 10^{77}}{33{,}86 \text{ x } 10^{15}} \text{ Sekunden} \sim 3{,}426 \text{ x } 10^{60} \text{ Sekunden} \sim \mathbf{1{,}086 \text{ x } 10^{53} \text{ Jahre}}$$

um erfolgreich alle Kombinationen zu testen. Unabhängig davon, dass der Supercomputer nicht so schnell wie vereinfacht gerechnet verarbeiten kann, ist nach aktuellen Maßstäben und State-of-the-Art-Technologien mit Gewissheit davon auszugehen, dass die gewählte 256-bit Verschlüsselung und somit die gesicherten Daten auf unserem OnlineBackup Server zu 100% sicher sind.

5 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.

6 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

6.1 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.

6.2 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.

6.3 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.

7 Überlegungen zur Thema Sicherheit bei Backup Software

Der Einsatz von Daten Backup-Produkten birgt die systemimmanenten Probleme, dass Daten

- dupliziert und an einem zusätzlichen Ort gespeichert werden,
- auf der Serverfestplatte geschützte Daten sehr oft unverschlüsselt auf Bänder etc. gespeichert werden,
- eine möglicherweise ausgeklügelte Zugriffsschutz-Strategie für unterschiedliche Benutzergruppen durch das alle Systeme umfassende Firmen-Backup ausgehebelt wird.

So werden in Organisationen häufig unterschiedliche Berechtigungsstrukturen für Benutzer, Administratoren, Management an den lokalen Servern festgelegt. Durch den Einsatz typischer Backup-Produkte werden die Daten doch wieder von allen unterschiedlichen Berechtigungszonen auf Sicherungsmedien (Backup-Systeme, Bänder) kopiert. Die Wiederherstellung von Daten obliegt typischerweise der IT-Administration, die nun doch wieder Berechtigungen quer über alle Berechtigungszonen erhält.

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.

Mit herkömmlichen Backup-Produkten lassen sich solche Szenarien nur mit relativ hohem Aufwand abbilden.

Außerdem wächst mit jeder Vervielfältigung von Daten und einer zusätzlichen Lagerung die potentielle Gefahr, dass diese Daten verloren gehen oder abgegriffen werden können.

Durch die Sicherheitsarchitektur von DataNoah lassen sich obige Sicherheitskonzepte sehr leicht realisieren. DataNoah lässt per se nur eine Archivierung von verschlüsselten Daten zu. Eine Ausnahme von dieser Regel ist nicht möglich. Dies bedeutet, dass Daten, die im DataNoah Rechenzentrum gespeichert sind oder Daten, die möglicherweise auf lokalen externen Festplatten gespeichert sind, und nicht berechtigte Dritte komplett wertlos sind.

DataNoah bietet von vornherein die Möglichkeit, die Datensicherung einerseits in verschiedene Backup Sets mit jeweils unterschiedlichen Verschlüsselungskennwörtern zu trennen und außerdem durch zwischen Verschlüsselungskennwörtern und Benutzerkennwörtern für die User Accounts zu unterscheiden. Dieses Konzept erlaubt eine viel differenzierte und sichere Backup-Strategie als dies viele typische Backup-Produkte bieten. So ist es möglich, dass z.B. die lokale IT-Administration zwar für die Überwachung das Backups zuständig ist, aber bestimmte Datenbereiche, die auch Administratoren nicht zugänglich sein sollten, nur mit

Verschlüsselungskennwörtern archiviert werden, die einer bestimmten Personengruppe vorbehalten ist.

Eine weitere, oft vernachlässigte Lücke in der Backup-Strategie stellen Laptops dar. Zwar werden typischerweise unternehmenskritische Legacy-Anwendungen auf Servern ausgeführt, die einer Backup-Strategie unterliegen.

Allerdings werden in der Praxis – speziell auf Laptops des Managements – viele Daten „kurzfristig“ gespeichert, die nie Teil einer Backup-Strategie sind. Oftmals ist ein Backup dieser Daten vom Management nicht gewünscht, weil es sich um gemischt unternehmensinterne und private Daten handelt oder andererseits um so sensible Unternehmensdaten, dass die lokale IT-Administration auf diese Daten keinen Zugriff haben soll – auch und gerade nicht für das Backup.

Diese Lücke in der Backup-Strategie kann mit DataNoah sehr leicht und mit verlässlicher Datenschutz-Strategie geschlossen werden: Am Notebook wird die lokale DataNoah Software, typischerweise DataNoah Notebook, installiert. Die Software sichert Daten in das DataNoah Rechenzentrum wenn das Notebook eine Internet-Verbindung hat. Die Daten des Notebooks werden in einem eigenen Backup-Set mit eigenem Verschlüsselungskennwort gesichert. Die lokale IT-Administration kann zwar den Backup-Prozess überwachen, nicht aber Daten wiederherstellen.