



SICHERES ARCHIV

Den ROI des **Primärspeichers**
maximieren und **Daten schützen**

Einführung SPEICHEROPTIMIERUNG IST EIN MUSS

Aktive Daten nehmen lediglich zehn bis zwölf Prozent der Kapazität des Primärspeichers in Anspruch. Den Großteil des Speicherplatzes belegen somit Informationen, auf die 90 Tage oder länger kein Zugriff erfolgte.

Hinzu kommt, dass der Speicher auf die Leistungs-, Kapazitäts- und Verfügbarkeitsanforderungen der verschiedenen Datentypen abgestimmt werden muss. Hierzu zählt, selten genutzte Informationen von teurem, leistungsstarken Primär- auf kostengünstigeren und weniger performanten Sekundärspeicher zu verlagern. Die Freigabe von Kapazität und die Steigerung der Leistung maximiert den ROI des Primärspeichers. Indem die Menge der abzusichernden Daten verringert wird, lässt sich zudem das Backup-Zeitfenster verkürzen. Verbleiben ausschließlich tatsächlich benötigte Daten auf dem Primärspeicher, senkt dies letztlich die Kosten.

Aber halt: Wie lässt sich der Speicher optimieren und im gleichen Zug gewährleisten, dass Nutzer von ihnen gewünschte Daten weiterhin direkt auffinden? Und wie kann eine sichere Archivierung mögliche Datenverluste verhindern?



Inaktive Daten
Daten, auf die 90 Tage oder länger kein Zugriff erfolgte

HOFFNUNG IST KEIN GUTER BERATER

Die Menge und Vielfalt an Möglichkeiten, die Integrität von Daten zu verletzen, ist erschreckend. Diese reichen von einer durch Hard- oder Softwarefehler verursachten schleichenden Korruption über schädliche von Cyberkriminellen initiierte Angriffe bis hin zu menschlichen Fehlern wie dem versehentlichen Löschen oder Überschreiben von Daten. Um all diesen und vielen weiteren Gefahren wirksam zu begegnen, führt kein Weg an einer durchdachten Datenschutzstrategie vorbei, auf deren Basis sich vier entscheidende Fragen beantworten lassen:

- 1. Sind alle Dateien in einem Backup gesichert oder im Archiv gespeichert?**
- 2. Ist auch am externen Standort eine zweite Kopie aller Daten vorhanden?**
- 3. Wie ist es um die Datenintegrität der an verschiedenen Standorten gespeicherten Dateien bestellt?**
- 4. Welche Datei ist die richtige, insofern es Unterschiede gibt?**



Sie sind sich nicht sicher, ob Sie diese Fragen beantworten können? Keine Sorge, damit stehen Sie nicht alleine. Dies liegt in erster Linie daran, dass Standard-Archiv- oder Backup-Systeme für solche Abfragen erforderliche Informationen nicht ohne Weiteres zur Verfügung stellen können.

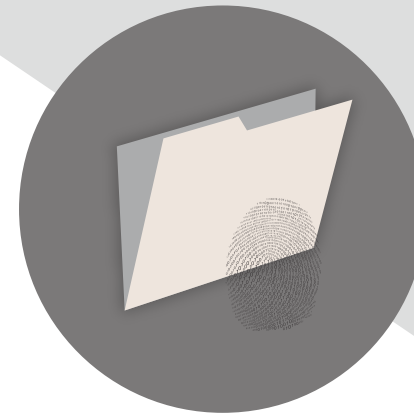
Allerdings können Sie in diesem Fall nur hoffen, dass die von Ihnen gewählten Datenschutzmaßnahmen greifen und nichts schief läuft. Das ist nicht nur eine risikoreiche Angelegenheit, sondern schlichtweg keine erfolgsversprechende Strategie.

Die Antwort auf diese Fragen — und tatsächlich einen Ausweg aus diesem Dilemma — geben eigens entwickelte sichere Archivlösungen. Diese sind von Grund auf darauf ausgelegt, den Schutz, die Integrität und Vertraulichkeit von Daten von dem Moment an sicherzustellen, an dem sie an das Archiv übergeben werden.

WIE SICH MIT EINEM SICHEREN ARCHIV DATEN AUF BEISPIELLOSE WEISE SCHÜTZEN LASSEN

Eine sichere Archivlösung weist jeder eingehenden Datei zunächst einen unverwechselbaren digitalen Fingerabdruck zu - ein Goldstandard, der dazu dient, die Integrität der Originaldatei zu wahren. Darauf folgend wird eine Kopie der Ursprungsdatei erzeugt und das Duplikat einschließlich des Inhalts und zugehöriger Metadaten abgelegt: entweder auf den Platten eines separaten RAID-Sets im lokalen Archivsystem oder auf einem sicheren Archivspeicher an einem externen Standort, beispielsweise am Hauptsitz des Unternehmens, in der Cloud etc.

Werden Dateien vom Primärspeicher in ein sicheres Archiv verschoben, bleibt auf dem System ein entsprechender Verweis erhalten. Dies ermöglicht Anwendern anders als bei einem konventionellen Backup, direkt auf benötigte Informationen zuzugreifen. Dabei spielte es keine Rolle, wo sich diese gerade befinden.



**Digitaler
Fingerabdruck**



Duplizierung

Da in einem sicheren Archivsystem redundante Datenkopien vorgehalten werden, müssen offene oder gerade verwendete Dateien nicht länger gesichert werden. Ebenso entfallen Wiederherstellungsvorgänge.

Die Aufbewahrung eines Duplikats von jeder übertragenen Originaldatei ermöglicht zudem, unverzichtbare vergleichende Dateianalysen auszuführen. Hierfür kommen zwei leistungsstarke Datenschutztechnologien zum Einsatz: Die **Dateiserialisierung** und der **digitale Fingerabdruck**.

1

2

3

5

7

6

4

Fehlende Datei

DATEISERIALISIERUNG UND PRÜFUNG

Dateikopien werden permanent auf ihre fortlaufende, eindeutige Seriennummer und ihre Integrität geprüft. Dadurch lässt sich ein deutlich besserer Datenschutz als mit gängigen für die Sicherung und Wiederherstellung von Daten verfügbaren Lösungen erzielen.

Jede im sicheren Archiv eingehende Datei erhält eine eindeutige Seriennummer (beiden Kopien - Original als auch Duplikat - wird dieselbe Seriennummer zugewiesen). Die Dateiserialisierung ermöglicht in regelmäßigen Abständen zu überprüfen, ob und an welcher Stelle jede Datei im sicheren Archiv sowohl am primären als auch am sekundären Standort (oftmals eine Außenstelle) vorhanden ist.

Ziel der Serialisierungsprüfung ist, die Datenverfügbarkeit zu verifizieren. Dadurch können IT-Verantwortliche die vorab erste und zweite gestellte Frage **“Sind alle meine Daten vorhanden?”** klar beantworten.

8

9

10

DIGITALER FINGERABDRUCK UND INTEGRITÄTSPRÜFUNG

In ähnlicher Weise wie bei der zuvor beschriebenen Dateiserialisierung, erzeugt ein sicheres Archiv für jede erfasste Datei und deren Kopie einen einzigartigen und unverwechselbaren "digitalen Fingerabdruck". Dieser dient dem System dazu, die Dateien in regelmäßigen Abständen auf ihre Integrität zu prüfen und sicherzustellen, dass keine Änderungen an den Daten vorgenommen wurden.

Beispielsweise lassen sich von einem Original nachfolgend erstellte und an einem externen Standort gespeicherte Kopien durch den Vergleich ihres digitalen Fingerabdrucks mit dem der Ursprungsversion auf ihre Korrektheit überprüfen. Moderne sichere Archivlösungen der Spitzenklasse nutzen zur Berechnung des digitalen Fingerabdrucks für jede Datei jeweils zwei Hash-Algorithmen: MD5 und SHA1.

Werden bei dem Prüfprozess jedoch modifizierte oder beschädigte Daten entdeckt, erfolgt eine Benachrichtigung und das Archiv ersetzt die fehlerhafte Datei automatisch durch ihre unversehrte Kopie.



Ziel des Prüfprozesses ist, die Integrität der Daten zu verifizieren. Dies ermöglicht IT-Verantwortlichen, die vorab gestellte dritte und vierte Frage **“Sind alle meine Daten unversehrt?”** mit einem “Ja” zu beantworten.

Dateiserialisierungs- und -integritätsprüfungen sind zwei zentrale Technologien eines wirklich sicheren Archivsystems. Doch ergänzend hierzu wartet Nexsan AssureonTM mit vielen weiteren für ein sicheres Archiv unerlässlichen Datenschutzfunktionen auf.

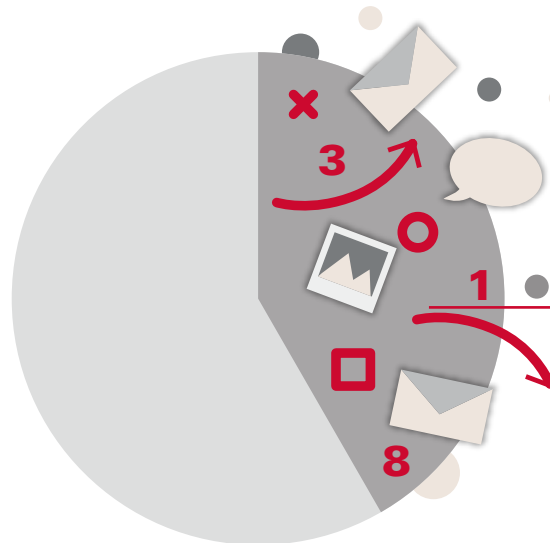
DATENSCHUTZ IN ZWEIGSTELLEN LEICHT GEMACHT

Während 2013 rund 40 Prozent aller Daten im digitalen Universum Schutz benötigten, wurden weniger als 20 Prozent tatsächlich abgesichert.*

In Außenstellen oder Niederlassungen gespeicherte Dateien umfassend zu schützen, stellt in den meisten Fällen eine Herausforderung dar. Oftmals scheitert es daran, dass möglicherweise keine oder nur wenige IT-Mitarbeiter vor Ort zur Verfügung stehen, die diese Aufgabe übernehmen können. Mit dem Einsatz eines sicheren Assureon-Archivs am Unternehmens Hauptsitz in Kombination mit per NAS und CIFS freigegebenen Assureon Edge NAS-Systemen in jeder Niederlassung lässt sich dieses Problem auf einfache und wirtschaftliche Art lösen.

Alle auf den Assureon Edge-Systemen in den einzelnen Außenstellen gespeicherten Daten lassen sich sicher an das zentrale Assureon-Speichersystem am Hauptsitz übermitteln und dort archivieren.

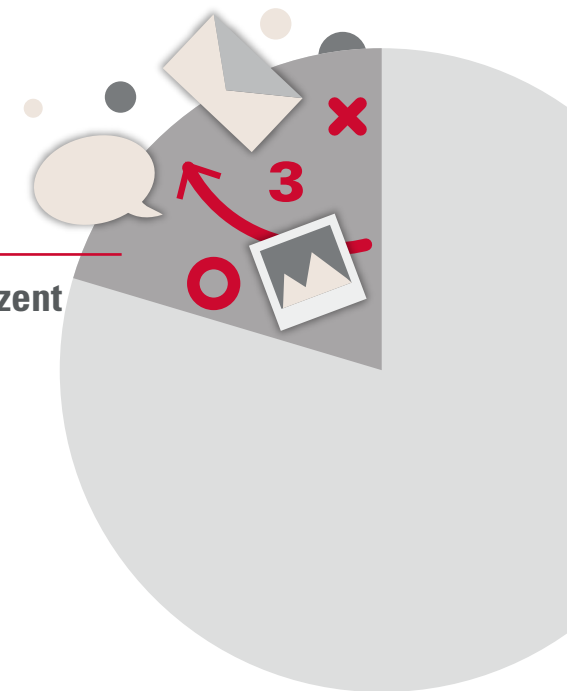
NEXSANTM
by imation



40 Prozent der Informationen erfordern einen umfassenden Datenschutz



Doch nur 20 Prozent sind tatsächlich abgesichert

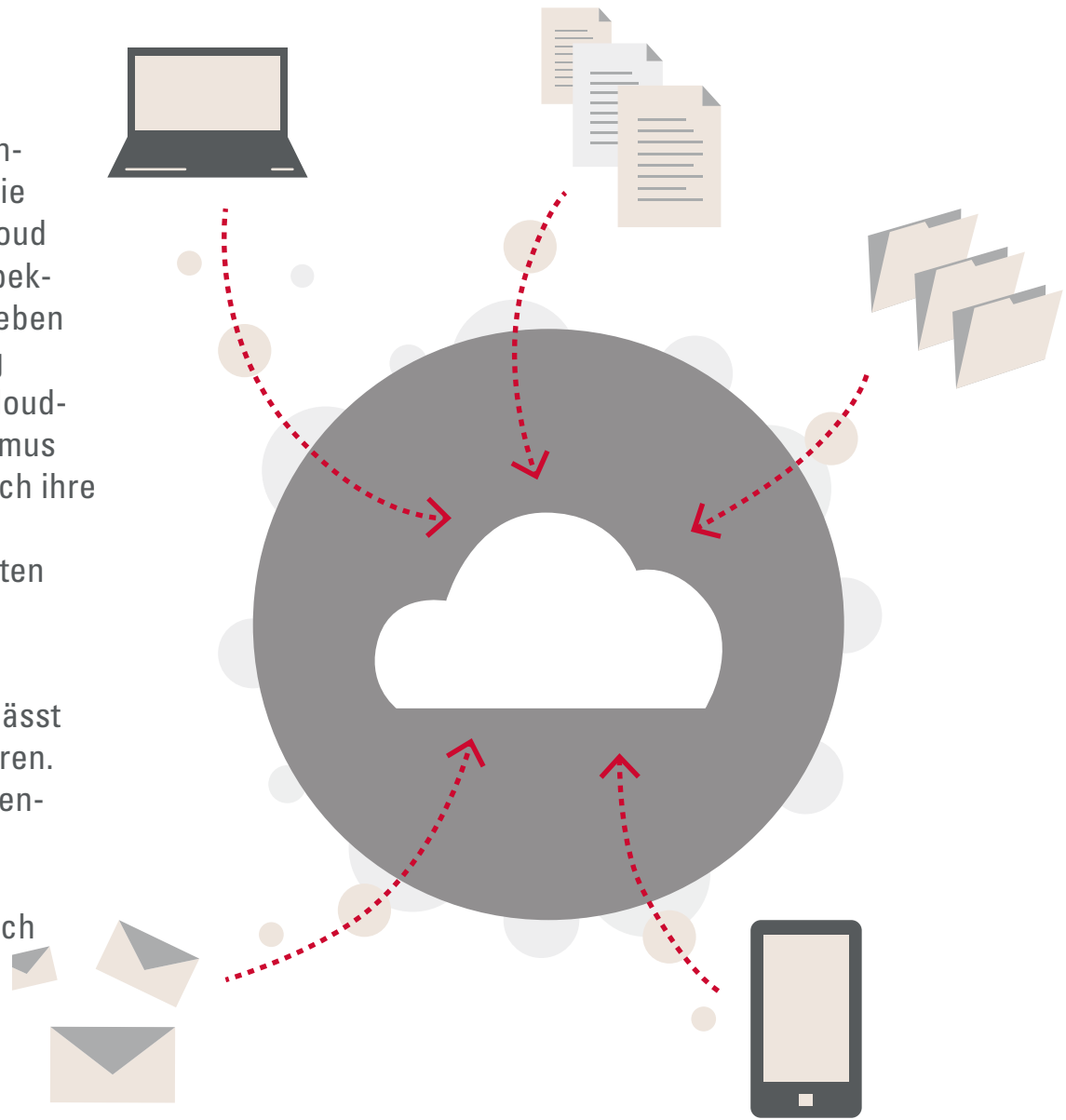


Alternativ hierzu lässt sich ebenso ein Assureon-Client auf einem in der Niederlassung betriebenen Windows-Server installieren. Dieser überträgt ausgewählte Verzeichnisse und Dateien an das am Hauptstandort des Unternehmens eingesetzte Assureon-System.

FÜR DEN EINSATZ MIT CLOUD-SPEICHERN KONZIPIERT

Die Assureon-Archivspeicher wurden als mandantenfähige Systeme entwickelt. Anbieter, die Archivspeicher als Dienstleistung über die Cloud bereitstellen, profitieren von einem breiten Spektrum an Sicherheitsfunktionen. Hierzu zählt neben einer zertifikatsbasierenden Authentifizierung unter anderem auch, dass die Dateien jedes Cloud-Service-Kunden mittels des AES-256-Algorithmus separat verschlüsselt werden. Zudem lässt sich ihre Speichernutzung genau nachvollziehen und Anbieter können die hierzu in Standardberichten enthaltenen Informationen einfach in ihr Abrechnungssystem importieren.

Beim Einsatz in privaten Cloud-Umgebungen lässt sich Assureon als virtuelles Archiv konfigurieren. Dies ermöglicht, von mehreren sicheren Anwendungen, Abteilungen oder gar verschiedenen Unternehmen erzeugte Daten individuell zu verschlüsseln und sowohl physikalisch als auch logisch vollständig separat zu speichern.



OPTIMAL FÜR DIE SPEICHERUNG WERTVOLLER DATEN

Anfangen von Computertomographie- (CT) und Positronen-Emissions-Tomographie- (PET) Scans über die Magnetresonanztomographie sowie Elektrokardiographie bis hin zu Laborberichten, elektronischen Patientenakten und kooperativen Versorgungsstrukturen: im Gesundheitswesen tätige Anbieter müssen gewaltig ansteigende Mengen an Daten verwalten.

Die Assureon-Systeme sind speziell darauf ausgelegt, lebenswichtige, unersetzliche Informationen umfassend zu schützen. Die branchenweit einzigartigen Lösungen verbinden auf beispiellose Weise das Beste aus zwei Welten: Die Vertraulichkeit, Integrität und Langlebigkeit eines sicheren Archivsystems mit bewährter Festplattentechnologie für den Hochgeschwindigkeitszugriff auf Daten. Darüber hinaus erfüllen die Systeme strengste gesetzliche Auflagen und damit die Bedingungen, die vor allem beim Einsatz im Gesundheitswesen an Archivspeicher gestellt werden.



Dementsprechend überrascht es kaum, dass die Assureon-Systeme genau in diesem Segment zu den meist genutzten Speichern zählen. Aber auch in Einrichtungen von Bund und Ländern sowie Kommunalverwaltungen sind die Nexsan-Produkte häufig anzutreffen. Darüber hinaus eignen sie sich für den Einsatz in Unternehmen, die auf den umfassenden und zuverlässigen Schutz der bei ihnen gespeicherten Daten angewiesen sind. Daher vertrauen Call Center sowie Firmen, die Videoüberwachungssysteme einsetzen oder an mehreren Standorten vertreten sind, immer häufiger auf die Assureon-Archivsysteme.

DAS SICHERE ASSUREON-ARCHIV: GESCHÜTZT, EFFIZIENT UND CLOUD-FÄHIG

Die Menge an unstrukturierten und strukturierten Daten nimmt weiterhin explosionsartig zu. Da auf einen Großteil der Informationen jedoch nur selten zugegriffen wird, ist es weder unter Performance-Aspekten noch unter wirtschaftlichen Gesichtspunkten sinnvoll, diese auf kostspieligen Primärspeichern vorzuhalten. Die sicheren Nexsan Assureon-Archivsysteme sind hingegen eigens dafür entwickelt, gespeicherte Daten auf beispiellose Weise zu schützen, sei es für Tage oder Jahrzehnte.

GESCHÜTZT

Datenintegrität: Bei jeder Speicherung einer Datei wird für diese unter Verwendung des MD5- und SHA1-Algorithmus ein eindeutiger Fingerabdruck erzeugt, der ihren Inhalt und ihre Metadaten enthält. Nachträgliche Änderungen des Dateiversionsverlaufs und des Inhalts werden dadurch ausgeschlossen. Alle 90 Tage wird die Integrität jeder Datei durch den Abgleich mit dem originalen digitalen Fingerabdruck geprüft.

Datenverfügbarkeit: Jeder Datei ist eine fortlaufende und eindeutige Seriennummer zugeordnet. Über diese lassen sich verschwundene Dateien schnell wieder auffinden. Ebenso kann festgestellt werden, ob Daten unberechtigt hinzugefügt wurden. Alle 90 Tage wird geprüft, ob noch jede Datei im Archiv vorhanden ist.

Dateiredundanz: Von jeder Datei werden jeweils zwei Kopien zusammen mit ihren Fingerabdrücken auf Assureon abgespeichert. Die zweite Kopie liegt entweder auf den Festplatten eines separaten RAID-Sets im gleichen System oder aber auf einem Assureon-Speicher, der an einem externen Standort zum Einsatz kommt.

EFFIZIENT

Verbesserter ROI: Die Verlagerung selten genutzter Dateien auf ein Assureon-Archiv bietet zahlreiche Vorteile: auf dem Primärspeicher steht wieder mehr Kapazität zur Verfügung, das System arbeitet mit höherer Performance und für das Backup angesetzte Zeitfenster lassen sich immens verkürzen.

Schluß mit Backups: Da jeweils zwei Kopien einer Datei im sicheren Archiv gespeichert werden, gehören teure Datensicherungs- und Wiederherstellungsprozesse der Vergangenheit an.

Schnelle Wiederherstellung: Bei der Wiederherstellung von Dateien werden anstelle der eigentlichen Dateiinhalte lediglich winzig kleine und damit wenig Speicherplatz belegende Verknüpfungen ersetzt. Dies ermöglicht IT-Verantwortlichen selbst anspruchsvollste Recovery-Point-Objective- (RPO) und Recovery-Time-Objective- (RTO) Ziele zu erfüllen.

CLOUD-FÄHIG

Mandantenfähig: Die Mehrmandantenfähigkeit von Assureon ermöglicht Anbietern von Cloud-Diensten, hochsichere Archivierungsdienste als Dienstleistung ("Archive as a Service", kurz AaaS) anzubieten. Jede Datei wird individuell verschlüsselt und die Speicherung von Daten erfolgt sowohl logisch als auch physikalisch voneinander getrennt.

Online-Archiv: Ein vor Ort eingesetzter Assureon-Speicher kann Daten in einen über die Cloud angebotenen Archivdienst replizieren. In privaten Cloud-Umgebungen unterstützt Assureon die One-to-One- und die Many-to-One-Replikation.

Kurz gesagt lassen sich durch den Einsatz von Assureon, die mit dem Betrieb des Primärspeichers verbundenen Kosten senken, ohne Kompromisse in Sachen Datenschutz einzugehen zu müssen.

ÜBER IMATION

Imation ist ein weltweit tätiger Hersteller von Speichermedien und Datenschutzlösungen. Zu den von Imation angebotenen Nexsan-Produkten zählen Solid-State-Storage-optimierte hybride Unified-Storage-Systeme, sichere automatisierte Archivlösungen und für den Unternehmenseinsatz entwickelte hochdichte Speicherarrays. Nexsan-Systeme eignen sich ideal für den Einsatz mit geschäftskritischen Virtualisierungs-, Cloud-, Collaboration- und Datenbankanwendungen. Darüber hinaus stehen energieeffiziente, hochdichte Speicher für Backup- und Archivierungszwecke zur Verfügung. Weltweit wurden seit 1999 mehr als 33.000 Nexsan-Systeme bei über 11.000 Kunden installiert. Die Nexsan-Speicher sind über das weltweite Vertriebspartnernetz des Herstellers erhältlich, zu dem Cloud-Service-Provider, Value-Add-Reseller und Lösungsintegratoren zählen. Weitere Informationen sind im Internet unter der Webadresse www.imation.com/nexsan abrufbar.