WHITEPAPER

NEXSAN™
by imation

SICHERES ARCHIV

DEN ROI DES PRIMÄR-SPEICHERS MAXIMIEREN & DATEN SCHÜTZEN

imation

EINLEITUNG

"Mit weniger mehr erreichen", so lautet das Gebot der Stunde. Diese Vorgabe müssen IT-Verantwortliche heute bei dem Versuch, mit immer knapperen Budgets das scheinbar grenzenlose Wachstum an unstrukturierten und strukturierten Daten zu bewältigen, tagtäglich erfüllen. Dass der Betrieb eines sich rasch füllenden (und dadurch verlangsamtem) Primärspeichers die Verlagerung weniger häufig genutzter Daten auf ein wirtschaftlicheres Storage-System erfordert, steht dabei außer Frage (siehe Abbildung 1 unten).

Speicheroptimierung bedeutet, Storage genau auf die Anforderungen abzustimmen, die Daten an Leistung, Kapazität und Verfügbarkeit stellen. Dies bringt mit sich, selten genutzte Daten von teurem, leistungsstarkem Primärspeicher auf kostengünstigere, weniger performante Sekundärspeicher zu verlagern. Die Freigabe von Kapazität, die Steigerung der Leistung, die Verkürzung des Backup-Fensters und die Sicherstellung, dass alle tatsächlich benötigten Daten auf dem Primärspeicher verbleiben, maximiert dessen ROI. So weit so gut . . .

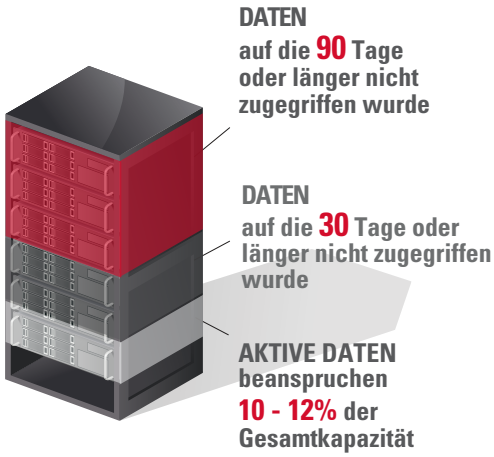

ABBILDUNG 1
NUR EIN KLEINER PROZENTSATZ DER AUF EINEM TYPISCHEN PRIMÄRSPEICHER ABGELEGTEN DATEN IST LAUFEND AKTIV

ARCHIV, BACKUPS . . . UND DATENVERLUST

Ohne eine gute Planung stellt die Verlagerung von Daten auf einen Sekundärspeicher IT-Verantwortliche vor neue Herausforderungen: die Administration verursacht Kopfzerbrechen (wie und wohin sollen seltener genutzte Informationen verschoben werden und wie können Anwender gewünschte Daten wieder auffinden, ohne die IT-Abteilung einzuschalten), es entstehen zusätzliche Kosten für den Einsatz und die Verwaltung einer weiteren Backup-Lösung . . . doch halt, warum das?

Da der Sekundärspeicher als **Archiv** dient (Storage für die dauerhafte Aufbewahrung von und den künftigen Verweis auf Daten, die im täglichen Geschäftsbetrieb nicht länger aktiv genutzt werden), sind hier **Original**-Dateien abgelegt, die von ihrem ursprünglichen Standort (in diesem Fall vom Primärspeicher) **verlagert** und zur sicheren Aufbewahrung an anderer Stelle gespeichert werden. Deshalb sind eine oder mehr **Kopien** der archivierten Daten erforderlich, die sich für die Wiederherstellung der Originale nutzen lassen, sollten diese verloren gehen oder irreparabel sein.

Was uns zum eigentlichen Punkt bringt: Datenverlust! Ein zentrales Thema, das im Mittelpunkt jeder Initiative zur Optimierung des Speichers und der Archivierung stehen muss.

Auf dem Primärspeicher abgelegte aktive Dateien werden fortlaufend abgerufen und geöffnet. Dadurch ist schnell ersichtlich, ob diese beschädigt sind oder fehlen. Ferner verschlimmert die häufige Erstellung von Snapshots oder Sicherung von Primärdaten jedes mit verschwundenen oder nicht lesbaren Informationen verbundene Problem. Doch wie verhält es sich mit entweder im Primärspeicher oder Archiv abgelegten Dateien, auf die seltener zugegriffen wird? Wochen, Monate oder gar Jahre können verstreichen,

Imation EMEA, Planeetbaan 4, 2132 HZ Hoofddorp, Niederlande | p. +31 23.521.2000 | www.imation.eu/nexsan

bis dem Unternehmen auffällt, dass eine Datei beschädigt ... oder einfach verschwunden ist.

Hierbei handelt es sich um ein grundlegendes konventionellen Speicherlösungen innewohnendes Problem. Auf dieses stoßen IT-Verantwortliche in der Regel erst dann, wenn sich eine Datei nicht mehr öffnen lässt oder überhaupt nicht mehr aufzufinden ist. Dabei gilt zu bedenken, dass eine nach der Beschädigung oder dem Verlust der Daten vorgenommene Sicherung keineswegs dazu beiträgt, die Datei zu reparieren oder ihren Originalzustand wiederherzustellen.

DAS PRINZIP HOFFNUNG IST KEINE GUTE STRATEGIE

In einer richtungsweisenden Studie veröffentlichte das renommierte Zentrum für physikalische Grundlagenforschung CERN im Jahr 2007 die Ergebnisse von Tests, in deren Rahmen das Verhalten von 3.000 an RAID-Subsysteme angeschlossenen Servern untersucht wurde[1]. In drei Wochen wurden dabei bei 17 Prozent der RAID-Arrays 500 beschädigte Dateien gefunden. Statistisch kommen somit korrupte Daten in einer von 1.500 Dateien vor.

Oracle publizierte im Februar 2013 einen Beitrag zu einem ähnlichen Thema, der sich mit der "Gefahr der schleichenden Datenkorruption"[2] und vorbeugenden Maßnahmen befasste. In diesem Zusammenhang wurde darauf hingewiesen, dass "[dies] jederzeit ohne jegliche Vorwarnung eintreten kann. Der Datenverlust sich jedoch nicht auf böswillige Aktivitäten, sondern auf das Versagen von Komponenten oder unbeabsichtigten administrativen Aktionen zurückführen lässt. Die "stille" Datenkorruption ist demgemäß weniger Ergebnis eines gescheiterten I/O-Vorgangs. Vielmehr wird sie durch das Lesen oder Schreiben ungültiger Daten verursacht. Diese Art der Beschädigung stellt die bei weitem dramatischste Form dar und lässt sich ohne **durchgängige Integritätsprüfungen** nicht effektiv ausfindig machen.

Die Menge und Vielfalt an Möglichkeiten, die Integrität von Daten zu verletzen, ist erschreckend. Hardware- und Softwarefehler, schädliche von Cyberkriminellen initiierte Angriffe oder menschliche Fehler wie das versehentliche Löschen oder Überschreiben von Daten und vieles weitere mehr: all dies kann zur schleichenden Korruption von Daten beitragen. Um dem zu begegnen, setzen viel zu viele Rechenzentrumsverantwortliche nach wie vor auf eine wenig erfolgversprechende Strategie . . . auf das Prinzip Hoffnung.

[1]Datenintegrität, Bernd Panzer-Steindel, CERN/IT Ausarbeitung Version 1.3 8., April 2007

[2]"How to Prevent Silent Data Corruption", Martin Petersen und Sonny Singh, Veröffentlichungsdatum: Februar 2013, Link: http://www.oracle.com/technetwork/articles/servers-storage-admin/silent-data-corruption-1911480.html

Imation EMEA, Planeetbaan 4, 2132 HZ Hoofddorp, Niederlande | p. +31 23.521.2000 | www.imation.eu/nexsan

Solange sie keine Antworten auf die folgenden vier entscheidenden Fragen finden, können sie bei dem von ihnen in punkto Datenschutz eingeschlagenen Weg nur hoffen, dass nichts schief läuft:

1. **Wie lässt sich feststellen, dass alle Dateien in einem Backup gesichert oder im Archiv gespeichert sind?**
2. **Wie lässt sich feststellen, ob auch am externen Standort eine zweite Kopie aller Dateien vorhanden ist?**
3. **In welchem Zustand (Integrität) befinden sich die an den verschiedenen Standorten gespeicherten Dateien?**
4. **Falls sich die Dateien unterscheiden, welche davon ist dann die richtige?**

Kommen Standard-Archiv- oder Backup-Systeme zum Einsatz, können IT-Verantwortliche diese Fragen schlicht und ergreifend nicht beantworten. Dies liegt in erster Linie daran, dass für solche Abfragen erforderliche Informationen nicht ohne Weiteres bereitstehen. Gängige Archiv- und Backup-Lösungen bieten meist nicht die Möglichkeit, die Verfügbarkeit oder den Zustand jeder einzelnen Datei fortlaufend zu überwachen. Ihr Vorhandensein und ihre Integrität auf manuelle Weise zu überprüfen, ist praktisch unmöglich. Denn hierfür müssten Millionen oder vielleicht auch Milliarden Dateien einzeln geöffnet und eingesehen werden.

Die Antwort auf diese Fragen — und tatsächlich einen Ausweg aus diesem Dilemma — geben speziell für diesen Zweck 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

Wie bereits festgestellt, sind durchgängige Integritätsprüfungen der einzige Weg, um beschädigte Daten aufzudecken, beziehungsweise eine schleichende Korruption zu vermeiden. Jede Archivlösung ohne diese Funktionalität kann nicht glaubhaft von sich behaupten, "sicher" zu sein. Vielmehr fehlt es an den nötigen Mitteln, um Daten umfassend zu schützen.

Eine sichere Archivlösung weist jeder eingehenden Datei zunächst einen unverwechselbaren digitalen Fingerabdruck zu - ein Goldstandard, der dazu dient, die Integrität der Originaldatei zu wahren. Darauffolgend wird eine Kopie der Ursprungsdatei erzeugt und das Duplikat einschließlich des Inhalts und zugehöriger Metadaten abgelegt: entweder auf den Platten eines separaten

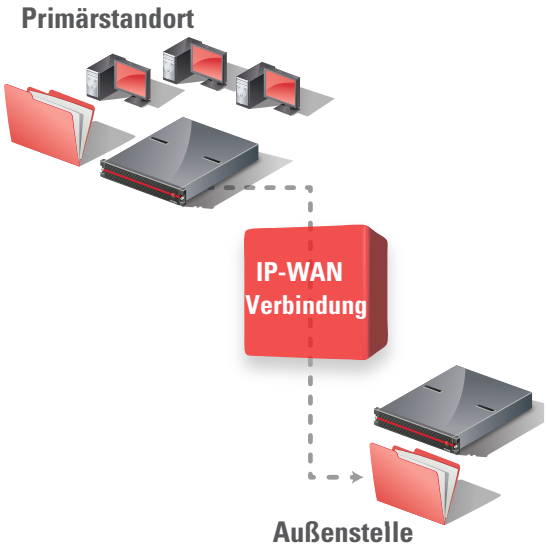

ABBILDUNG 2
EIN SICHERES ARCHIV BEWAHRT AUTOMATISCH ZWEI KOPIEN JEDER DATEI AUF, ENTWEDER LOKAL ODER AN EINEM EXTERNEN STANDORT.

RAID-Sets im lokalen Archivsystem oder auf einem sicheren Archivspeicher an einem externen Standort, beispielsweise am Hauptsitz des Unternehmen, in der Cloud etc. (siehe Abbildung 2 links).

Werden Dateien von dem Primärspeichersystem in das sichere Archiv verlagert, sollte auf letzterem ein Verweis erhalten bleiben. Dies ermöglicht Anwendern, auf gerade benötigte Informationen unmittelbar zuzugreifen (anders als bei einem gängigen Backup) und sorgt für Transparenz. Darüber hinaus lässt sich dadurch sicherstellen, dass Nutzer das Archiv nicht direkt durchsuchen oder sonstige Aktionen durchführen können. Ergebnis ist, dass Daten zu jedem beliebigen Zeitpunkt umfassend geschützt sind.

Da sichere Archivlösungen von jeder übertragenen Originaldatei eine Kopie aufbewahren, lassen sich vergleichende Dateianalysen ausführen. Hierfür kommen zwei leistungsstarke, den Schutz der Daten sicherstellende Techniken zum Einsatz::

- Die Dateiserialisierung
- Der digitale Fingerabdruck

Da in einem sicheren Archivsystem redundante Datenkopien vorgehalten werden, entfallen die **Sicherung offener oder gerader genutzter Dateien ebenso wie Wiederherstellungsvorgänge.** Darüber hinaus werden die Dateien permanent auf ihre fortlaufende, eindeutige Seriennummer und auf ihre Integrität geprüft. (siehe unten). Dadurch lässt sich ein deutlich besserer Datenschutz als mit gängigen für die Sicherung- und Wiederherstellung von Daten verfügbaren Lösungen erzielen.

DATEISERIALISIERUNG UND PRÜFUNG

Idealerweise wird jeder im sicheren Archiv gespeicherten Datei eine eindeutige Seriennummer zugewiesen (beide Dateikopien - Orginal als auch Duplikat - erhalten die gleiche Seriennummer). 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. Die bei einer sicheren Archivlösung genutzte Dateiserialisierung und Überprüfung ist mit den bei Unternehmen eingesetzten Kennzeichnungsverfahren und Nachverfolgungssystemem vergleichbar, mit denen sie für ihr Geschäftsergebnis entscheidende Sachanlagen wie PCs, Server oder Industriewerkzeuge klassifizieren und steuern.

Beispielsweise nutzt ein sicheres Archiv die Seriennummern, um zu prüfen, dass sich die Millionen auf den Festplatten des primären Archivsystems gespeicherten Daten immer noch an Ort und Stelle befinden. Ebenso, dass ihre Kopien weiterhin auf den Platten des Sekundärarchivs liegen. Wird eine fehlende Datei entdeckt, benachrichtigt das System den Administrator und ersetzt diese automatisch durch die serialisierte redundante Kopie (siehe Abbildung 3 unten).

ABBILDUNG 3
VERSCHWUNDENE DATEIEN LASSEN SICH ÜBER DIE IHNEN ZUGEORDNETE EINDEUTIGE SERIENNUMMER SCHNELL WIEDERAUFFINDEN.

ZUSAMMENFASSUNG SERIALISIERUNGSPRÜFUNG:

- Im sicheren Archiv eingehende Dateien erhalten eine eindeutige Seriennummer.
- In regelmäßigen Abständen wird überprüft, ob jede der eingangs gespeicherten Dateien noch im Archiv vorhanden ist.
- Es werden sowohl das Primär- als auch das Sekundärarchiv geprüft.
- Fehlende Daten werden gemeldet und die Verfügbarkeit von Dateien geprüft.

Ziel der Serialisierungsprüfung ist, die Datenverfügbarkeit zu verifizieren. Dies ermöglicht IT-Verantwortlichen, eine eindeutige Antwort auf den in der ersten und zweiten vorstehend formulierten Frage angesprochenen Punkt ***"Sind alle meine Daten vorhanden?"*** zu geben.

Imation EMEA, Planeetbaan 4, 2132 HZ Hoofddorp, Niederlande | p. +31 23.521.2000 | www.imation.eu/nexsan

DIGITALER FINGERABDRUCK UND INTEGRITÄTSPRÜFUNG

Um die Datenintegrität zu garantieren, wird bei einem sicheren Archiv für jede eingehende Datei und der von ihr erstellten Kopie ein eindeutiger "digitaler Fingerabdruck" erzeugt. Weitere darauffolgende und beispielsweise an einem externen Standort gespeicherte Duplikate des Originals lassen sich durch den Vergleich ihres digitalen Fingerabdrucks mit dem der Ursprungsversion auf ihre Korrektheit überprüfen. Moderne sichere Archivlösungen der Spitzenklasse verwenden zur Berechnung des digitalen Fingerabdrucks für jede Datei jeweils zwei Hash-Algorithmen: MD5 und SHA1.

In ähnlicher Weise wie bei der vorstehend beschriebenen Dateiserialisierungsprüfung kann das Archiv mittels der Fingerabdrücke in regelmäßigen Abständen die Integrität jeder Datei kontrollieren. Stimmen die Hash-Werte beim Vergleich mit dem ursprünglichen Referenzwert überein, erfolgte keine Änderung (zum Beispiel in Folge der schleichenden Datenkorruption, aufgrund von Festplattenfehlern, Viren, unberechtigten Zugriffen oder Replikationsfehlern). Werden bei dem Prüfprozess jedoch modifizierte oder beschädigte Daten entdeckt, erfolgt eine Benachrichtigung und das Archiv ersetzt die fehlerhafte Datei durch ihre unversehrte Kopie (siehe Abbildung 4 unten).

ABBILDUNG 4
EINDEUTIGER DIGITALER FINGERABDRUCK ERMÖGLICHT IN WIEDERKEHRENDEN ABSTÄNDEN ZU PRÜFEN, OB DATEIEN BESCHÄDIGT SIND

ZUSAMMENFASSUNG INTEGRITÄTSPRÜFUNG:

- Jedes Mal, wenn eine Datei im sicheren Archiv erfasst oder erneut gespeichert wird, erhält sie einen eindeutigen und unverwechselbaren Fingerabdruck.
- Anhand des Vergleichs der digitalen Fingerabdrücke wird geprüft, dass die Datei nicht geändert wurde (zum Beispiel in Folge der schleichenden Datenkorruption, aufgrund von Festplattenfehlern, Viren, unberechtigten Zugriffen oder Replikationsfehlern).
- Meldet beschädigte Daten und repariert diese.
- Prüft die Datenintegrität.

Imation EMEA, Planeetbaan 4, 2132 HZ Hoofddorp, Niederlande | p. +31 23.521.2000 | www.imation.eu/nexsan

Archiv-Systeme spielen bei der Umsetzung wirtschaftlicher Speicherkonzepte eine zentrale Rolle.

2014 entwickeln sich sichere Archivspeicher zunehmend zu einer Investition, die CIOs als strategisch ansehen. Ihr Einsatz verspricht, Daten wirtschaftlicher als bisher zu speichern, aufzubewahren und bereitzustellen.

"Active Archive: Top Five Data Predictions for 2014", David Cerf, Active Archive Alliance.

Intelligenter ausgelegte Speichersysteme verdoppeln die Produktivität von Administratoren.

Durch die Funktionserweiterungen von Storage-Systemen verdoppelt sich bis 2016 bemessen auf einer Petabyte- pro-Vollzeitkraft-Basis die Produktivität von Speicheradministroren.

Gartner, Mai 2013: "Market Share Analysis: Attached Storage and Unified Storage, Worldwide, 2012".

Ziel des Prüfprozesses ist, die Integrität der Daten zu verifizieren. Dies ermöglicht IT-Verantwortlichen, eine positive Antwort auf den in der dritten und vierten vorstehend formulierten Frage angesprochenen Punkt ***"Sind alle meine Daten unversehrt?"*** zu geben.

Neben den vorangehend beschriebenen für ein wirklich sicheres Archivsystem zwei entscheidenden Technologien muss dieses über viele weitere Datenschutzfunktionen verfügen. Eine Archivlösung zu finden, die alle erforderlichen technischen Leistungsmerkmale aufweist, ist keine einfache Angelegenheit. Aber sicherlich kein Ding der Unmöglichkeit . . .

NEXSAN ASSUREON™: SICHERES ARCHIV, UMFASSENDER DATENSCHUTZ

Die zur Nexsan Assureon™-Famile zählenden Archivsysteme senken mit der Speicherung verbundene Kosten, indem Daten vom Primärspeicher gemäß festgelegter Regeln (Zugriffshäufigkeit, Alter etc.) auf sie verlagert und dedupliziert werden. Durch eine richtlinienbasierte Automatisierung lassen sich mit Assureon Ausmaß, Kosten und Komplexität von Backup-Prozessen vollständig aufheben oder stark einschränken, die für die Sicherung primärer oder selten genutzter Daten erforderlich sind.

Assureon-Systeme sind von Hause aus mandantenfähig ausgelegt und bieten ein breites Spektrum an Funktionen zur Erzeugung sicherer Kopien und Datenmigration sowie der dauerhaften Speicherung von Informationen. Darüber hinaus lassen sich beim Einsatz der Archivsysteme in öffentlichen oder privaten Cloud-Umgebungen Kosten anteilig in Rechnung stellen. Zahlreiche Verfahren zur Wahrung der Datenintegrität wie digitale Fingerabdrücke oder automatisierte "selbstheilende" Integritätsprüfungen stellen den Schutz wertvoller Daten sicher. Die in Assureon integrierten Sicherheitsfunktionen erfüllen sowohl unternehmensinterne als auch gesetzliche Vorgaben. Daher eignen sich die Archivsysteme hervorragend für den Einsatz in Unternehmen, die im Gesundheitswesen oder der Finanzwirtschaft tätig sind. Ebenso vertrauen Einrichtungen von Bund und Ländern sowie Kommunalverwaltungen gerne auf die Lösungen.

Im Gegensatz zu anderen Archivsystemen garantiert Assureon die Integrität der gespeicherten Daten durch den Einsatz vielfältiger Techniken. Hierzu zählen unter anderem die Dateiserialisierung, digitale Fingerabdrücke, Audit-Trails sowie Eigenkontrolle- und Selbstheilungs-Funktionen. Da Assureon jede eingehende Datei umgehend dupliziert, ist **die Sicherung von Daten nicht länger erforderlich.** Dadurch lassen sich mit wöchentlichen Vollsicherungen oder täglichen inkrementellen Backups in Verbindung stehende Ausgaben (Hardware, IT-Management sowie basierend auf der Kapazität pro Terabyte anfallende Kosten für Backup-Anwendungen) erheblich eindämmen.

Imation EMEA, Planeetbaan 4, 2132 HZ Hoofddorp, Niederlande | p. +31 23.521.2000 | www.imation.eu/nexsan

Fehlender Datenschutz

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

IDC: "The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things," April 2014.

Enormes Datenwachstum prognostiziert

Die weltweite Datenmenge wird bis 2020 um den Faktor zehn wachsen und damit von 4,4 Billionen auf 44 Billionen Gigabyte ansteigen. Damit verdoppelt sich der Umfang des digitalen Universums künftig alle zwei Jahre.

IDC: "The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things," April 2014.

Trotz der leistungsstarken Technologien, die das Fundament für den von Assureon gebotenen umfassenden Schutz der Daten legen, arbeitet das Archivsystem im Hintergrund nahezu unmerklich für den Anwender. Jede in das Archiv verschobene Datei wird auf dem Primärspeicher durch eine Verknüpfung ersetzt. Dadurch müssen sich Nutzer nicht in neue Prozesse einarbeiten, sondern können wie gewohnt und auf die ihnen vertraute Art und Weise auf benötigte Daten zugreifen.

DATENSCHUTZ IN ZWEIGSTELLEN LEICHT GEMACHT

Außenstellen oder Niederlassungen mit nur wenigen oder möglicherweise keinen IT-Mitarbeitern vor Ort, tun sich häufig mit der Aufgabe schwer, den umfassenden Schutz der bei ihnen gespeicherten Daten sicherzustellen. Mit dem Einsatz eines sicheren Assureon-Archivs am Unternehmenshauptsitz 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-Speichersystemam Hauptsitz übermitteln und dort archivieren. 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 Assureon-System am Primärstandort , wo sie archiviert werden.

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 die separate Verschlüsselung von Dateien mit dem AES-256-Algorithmus. Die Speichernutzung jedes einzelnen Cloud-Service-Kunden lässt sich genau nachvollziehen, Anbieter können die in den Standardberichten hierzu 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.

Imation EMEA, Planeetbaan 4, 2132 HZ Hoofddorp, Niederlande | p. +31 23.521.2000 | www.imation.eu/nexsan

OPTIMAL FÜR DIE SPEICHERUNG WERTVOLLER DATEN

Angefangen von Computertomographie- (CT) und Positronen-Emissions-Tomographie- (PET) Scans über die Magnetresonanztomographie sowie Elektrokardiographie bis hin zu Laborberichten, fortlaufenden elektronischen Patientenakten und kooperativen Versorgungsstrukturen: im Gesundheitswesen tätige Anbieter müssen heute eine gewaltige, stets zunehmende Menge an Daten verwalten. Die Assureon-Systeme sind speziell darauf ausgelegt, lebenswichtige, unersetzliche Informationen umfassend zu sichern. Assureon bietet das Beste aus beiden Welten: Die Vertraulichkeit, Integrität und Langlebigkeit eines sicheren Archivssystems und bewährte 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

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 so 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.

Imation EMEA, Planeetbaan 4, 2132 HZ Hoofddorp, Niederlande | p. +31 23.521.2000 | www.imation.eu/nexsan

EFFIZIENT:

- **Verbesserter ROI:** Die Verlagerung selten genutzer 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.

Imation EMEA, Planeetbaan 4, 2132 Hoofddorp, Niederlande | Tel.: +31 23.521.2000 | www.imation.eu/nexsan

FAZIT

Dass die Menge an unstrukturierten und strukturierten Daten auch künftig in rasantem Tempo zunimmt, steht außer Frage. Diese weiterhin auf kostspieligen Primärspeichern vorzuhalten, erscheint unter wirtschaftlichen Aspekten betrachtet daher als ein ineffizienter Ansatz. Dies liegt in erster Linie daran, dass ein Großteil der Daten nur selten genutzt wird und daher nicht die von Primärspeichern gebotene hohe Leistung benötigt. Ganz zu schweigen von den Kosten, die mit der Speicherung auf einem solch hochperformanten System einhergehen. Da nicht alle Daten gleicher Natur sind, setzen IT-Verantwortliche inzwischen auf das Prinzip der Speicheroptimierung. Davon versprechen sie sich, Storage besser auf die von Daten an Leistung, Kapazität und Konnektivität gestellten Anforderungen abstimmen zu können.

So verheißungsvoll dies auch klingen mag: bei der Verlagerung selten genutzter Daten von einem Primärspeicher auf einen Archivspeicher übersehen sie häufig einen entscheidenden Punkt: die Gefahr des Datenverlusts. Um dem vorzubeugen, bietet sich der Einsatz der sicheren Assureon-Archivlösungen von Nexsan an. Die Systeme sind von Grund auf so ausgelegt, dass sie archivierte Daten rundum schützen. Dabei spielt es keine Rolle, ob die Informationen nur für einige Tage oder Jahrzehnte gespeichert werden sollen. Kurz gesagt ermöglicht Assureon IT-Verantwortlichen, die mit dem Betrieb von Primärspeichern verbundenen Kosten zu senken, ohne dass sie sich noch länger über das Thema Datenschutz den Kopf zerbrechen müssen.

ÜBER IMATION

Imation ist ein weltweit tätiger Anbieter 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 Storage-Arrays. Nexsan-Speicher 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-Speichersysteme bei über 11.000 Kunden installiert. Die Nexsan-Systeme 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.

Imation EMEA, Planeetbaan 4, 2132 Hoofddorp, Niederlande | Tel.: +31 23.521.2000 | www.imation.eu/nexsan