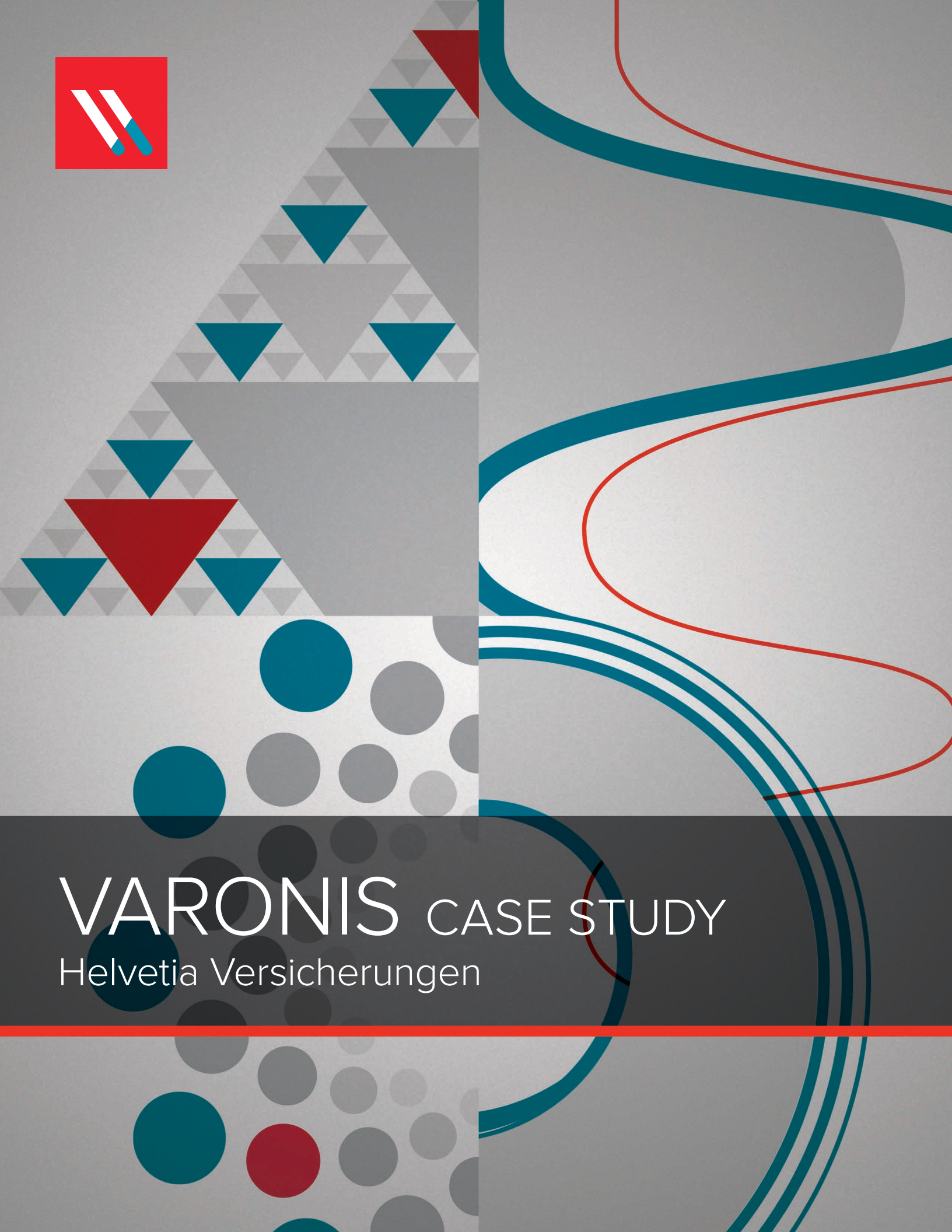

VARONIS CASE STUDY

Helvetia Versicherungen

„Mit Varonis verfügen wir über eine allumfassende Managementlösung für unsere Fileserver. Sie deckt sämtliche der von uns benötigten Funktionalitäten umfassend ab und kommt ohne Schnittstellen zu weiteren Systemen aus. Und letztendlich: jede Entscheidung, die für ein Unternehmen wie das unsrige besonders viel Tragweite hat, es ist immer ein „peoples business“. In diesem Fall waren das persönliche und fachliche Engagement des gesamten Teams mit ausschlaggebend für uns.“

– Michel Küng
Business Engineer Collaboration & IT-Arbeitsplatz und Mitglied der Direktion, Helvetia Versicherung, Schweiz.

DER KUNDE

Helvetia Versicherungen, www.helvetia.ch

ORT

Hauptsitz, Basel Schweiz, Gruppe europaweit tätig
Hauptsitz der Helvetia-Gruppe: St. Gallen, Schweiz

BRANCHE

Versicherungswirtschaft

HERAUSFORDERUNG

Berechtigungs- und Zugriffsmanagement optimieren und transparent nachvollziehbar machen, bi-direktionale Sicht auf Fileserver, Data Owner ermitteln und Berechtigungsvergabe aufgrund der Geschäftsprozesse einbeziehen, mit dem Ziel einer umfassenden Data Governance

DIE LÖSUNG

Varonis DatAdvantage und Varonis Data Privilege, geplant: Varonis DatAnyhwere

VORTEILE

- Umfassende Management-Lösung für Fileserver, sämtliche Funktionen integriert
- Komplette Transparenz hinsichtlich der Nutzer-, Gruppen- und Verzeichnisrechte auf Dateisystemen, SharePoint und Exchange inklusive Audit-Trail
- Automatisierte Übersichten zu Berechtigungen und Genehmigungsverfahren
- Durchsetzung interner Richtlinien in der Dateninfrastruktur, Einhaltung rechtlicher Vorgaben gewährleistet
- Einbindung von Data Ownern und Mitarbeitern in der Vergabe und Kontrolle von Berechtigungen

DER KUNDE

Die Helvetia hat eine lange Tradition: Sie ist in über 150 Jahren aus verschiedenen schweizerischen und ausländischen Versicherungsunternehmen zu einer erfolgreichen, europaweit präsenten Versicherungsgruppe gewachsen, die unter dem Leitsatz «Spitze bei Wachstum, Rentabilität und Kundentreue» agiert. Heute verfügt die Helvetia über Niederlassungen in der Schweiz, in Deutschland, Österreich, Spanien, Italien und Frankreich und organisiert Teile ihrer Investment- und Finanzierungsaktivitäten über Tochter- und Fondsgesellschaften in Luxemburg und Jersey. Der Hauptsitz der Gruppe befindet sich in St.Gallen, derjenige der Schweiz in Basel. Die Helvetia ist im Leben-, Schaden- und Rückversicherungsgeschäft aktiv und erbringt mit rund 5.200 Mitarbeitenden Dienstleistungen für mehr als 2.7 Millionen Kunden. Darüber hinaus engagiert sich die Helvetia auf vielfältige Weise für Umwelt und Gesellschaft. Die Namenaktien der Helvetia Holding werden an der Schweizer Börse SIX Swiss Exchange unter dem Kürzel HELN gehandelt.

EINLEITUNG

NUTZERGENERIERTE BIG DATA UND WAS DEN UMGANG MIT IHNEN ERSCHWERT

In den Terabytes an strukturierten und unstrukturierten Informationen liegt unzweifelhaft ein großes Potenzial. Geht die Datenproduktion allerdings in diesem Tempo weiter, kommen Firmen sehr schnell an einen Punkt, an dem sie Informationen nicht mehr als solche identifizieren und analysieren können. Die sogenannten nutzergenerierten Inhalte umfassen sämtliche Office-Dateien und E-Mails, die Business User tagtäglich erstellen: Präsentationen, Textverarbeitungsdokumente, Tabellenkalkulationen, Audio- und sonstige Dateien. Diese Daten werden über einen langen Zeitraum aufbewahrt, bearbeitet und zusätzliche Metadaten mit ihnen verknüpft. Unter Metadaten versteht man die Informationen zu einer Datei: wer hat sie erstellt, um welchen Dateityp handelt es sich, auf welchem System und in welchem Ordner ist sie gespeichert, wer hat sie geöffnet und wer kann darauf zugreifen. Schätzungsweise bis zu 80% aller Unternehmensdaten sind unstrukturierte Daten, auf die zu viele Personen zugreifen.

Oftmals haben Unternehmen auch die NTFS-Berechtigungen viel zu weit gesetzt. Dadurch können Mitarbeiter auf Daten zugreifen, auf die sie nicht zugreifen sollten. Die Zugriffsaktivitäten sind dann oftmals nicht ein Mal mehr nachzuvollziehen.

Die Datenflut ist so stark angewachsen, dass sie sich nicht mehr ohne komplexe, automatisierte Prozesse analysieren und verarbeiten lässt. Zahlreiche Organisationen, die Versicherungswirtschaft eingeschlossen, stehen folglich vor schwerwiegenden Problemen, die vor 15 Jahren bei kleineren, statischeren Datenmengen noch mühelos behoben werden konnten, jetzt aber unlösbar erscheinen.

Bei der Helvetia Schweiz hatte sich der Datenbestand in knapp zwei Jahren verdoppelt. Die zentralen Fragen: Wo befinden sich überhaupt kritische Daten? Wer greift darauf zu und wer sollte darauf zugreifen können? Wie sind die Berechtigungen vergeben?

Michel Küng, Business Engineer Collaboration & IT-Arbeitsplatz und Mitglied der Direktion:

„Wir haben nach einer Lösung gesucht, die alle technischen Funktionen bereitstellt, um den administrativen Aufwand bei der Berechtigungsvergabe zu reduzieren. Gleichzeitig sollte die Lösung auf die Business-Bedürfnisse unserer Branche zugeschnitten sein.“

DIE HERAUSFORDERUNG

Die Menge an nutzergenerierten Daten, darunter eine Vielzahl von vertraulichen Daten, stieg kontinuierlich an, bei der Helvetia in nur knapp zwei Jahren auf das Doppelte.

Den Überblick inklusive der vergebenen Berechtigungen zu behalten sowie Ereignisse nachzuvollziehen erwies sich als aufwendig bis unmöglich.

„Wir haben es, verglichen mit noch vor zehn Jahren mit einem explosiven Datenwachstum zu tun, darunter Unmengen an vertraulichen und hochsensiblen Kunden- und Geschäftsdaten. Einige Zahlen aus unserem Geschäftsalltag: auf unsere Fileserver-Cluster greifen etwa 3.200 Mitarbeiter zu. Fileserver sind damit noch vor Intranet und Wikis das zentrale Arbeitsinstrument. Die geschätzte Datenmenge beträgt etwa 5 Terabyte, die sich auf insgesamt etwa 960.000 Ordner verteilen. Das sind Zahlen, bei denen einem schon ein Mal ein bisschen schwindelig werden kann“, so Michel Küng.

„Die tatsächlichen Data Owner beziehungsweise diejenigen, die es hätten sein sollen, waren uns überwiegend nicht bekannt, und das wiederrum hat sich negativ darauf ausgewirkt wie die Berechtigungen vergeben worden sind. Zu einem großen Teil nämlich schlicht falsch. Wir konnten die Vergabe nicht transparent nachvollziehen, selbst nicht mit einem enormen manuellen Aufwand. Dazu kam, dass wir innerhalb unserer Active-Directory-Struktur nur mühsam ermitteln konnten, welche Mitarbeiter zu welchen Gruppen gehören, wo diese Gruppen genau zugeordnet sind und ob die betreffenden Gruppen den richtigen und ausschließlich diesen Mitarbeitern zugeordnet sind. Diese Fragen nicht befriedigend beantworten zu können, hatte bereits Probleme bei der Revision verursacht.“

EVALUIERUNG

„Die Helvetia-Versicherung hatte sich schon in der Vergangenheit mit dem Thema „automatisiertes Berechtigungsmanagement“ befasst, spruchreif wurde das Ganze allerdings erst im Dezember des letzten Jahres unter der Ägide von Michel Küng. Er griff das von Varonis erläuterte Thema wieder auf.

„Wir hatten schon einige pragmatische Ansätze geprüft, etwa fix vorgegebene Strukturen mit klaren Berechtigungen oder eine einfache Eigenentwicklung, die an das bestehende IAM-System angebunden werden sollte. Diese Ansätze sind in der Praxis allerdings schnell an ihre Grenzen gekommen. Entweder gingen sie an den geschäftlichen Erfordernissen und Bedürfnissen vorbei oder sie waren nur mit erheblichem Aufwand und einem ungewissen Ausgang realisierbar. Aufgrund dieser Erfahrungen haben wir uns intensiv mit der Lösung von Varonis auseinandergesetzt und DatAdvantage mit DataPrivilege evaluiert.“

Die Evaluierung startete im Februar 2014, Ende Juli 2014 ist die Implementierung abgeschlossen worden.

DIE LÖSUNG

In der knapp fünfmonatigen Evaluierungszeit wurden die Data-Governance-Lösungen DatAdvantage und DataPrivilege mit Blick auf das Anforderungsprofil ausführlich getestet.

Michel Küng: „Im Verlauf der Evaluierung hat sich gezeigt, dass die Varonis-Lösung technisch und im Hinblick auf unsere Geschäftsprozesse manuellen Lösungen und Eigenentwicklungen bei weitem überlegen ist.“

Primäres Ziel war es, sämtliche Berechtigungen sichtbar und nachvollziehbar zu machen, zu bereinigen und anschließend die tatsächlich zuständigen Data Owner, also die eigentlichen Business-Eigentümer der Daten wenn man so will, zu ermitteln. Sie sollten anschließend in die Lage versetzt werden, die Berechtigungen im jeweiligen Aufgaben- und Zuständigkeitsbereich selbst zu vergeben. Will man Berechtigungen konsolidieren und die kompletten Zugriffsaktivitäten nachvollziehen, hilft eine bi-direktionale Sicht auf die Filesystemberechtigungen, die Kenntnis der branchenspezifischen Geschäftsprozesse und Geschäftsmodelle eingeschlossen.

„Die Kernfunktionalitäten von DatAdvantage bilden das überzeugend ab, denn hier sieht man auf einen Blick welcher Benutzer auf welche Dateien und Ordner zugreifen kann“, so Küng weiter.

DatAdvantage nutzt statistische Prozesse, um Vorschläge für eine sinnvolle Berechtigungs-struktur zu machen, innerhalb derer es keine sogenannten „Überberechtigungen“ gibt. Die Software trägt verschiedene Arten von Informationen zusammen und setzt sie zueinander in Beziehung. So ermittelt sie beispielsweise wer am häufigsten auf einen bestimmten Ordner zugreift und Daten modifiziert hat. Sehr wahrscheinlich ist das dann der zuständige Data Owner.

Vielfach sind die sogenannten Metadaten der Schlüssel. Ein Metadaten-Framework sammelt im Hintergrund diese kritischen Metadaten beziehungsweise generiert sie dort wo sie noch nicht existieren. Diese Daten werden zusammengeführt, analysiert und für den zuständigen IT-Administrator auf einer dynamischen Oberfläche angezeigt. Sind die Dateneigentümer eindeutig identifiziert, treffen sie selbst, und nicht mehr die IT-Abteilung, sachkundige Autorisierungsentscheidungen. Die Data Owner erstellen dann genau die Berechtigungen, die den Geschäftsprozessen entsprechen. Wenn die Dateifreigaben in einem geordneten Rahmen verlaufen, ist es wichtig, sie auch weiterhin unter Kontrolle zu behalten. Dazu werden alle Ereignisse kontinuierlich auf Veränderungen hin überwacht. Etwas, das in oder für Unternehmen häufig innerhalb der Auditing-Anforderungen festgelegt ist.

„In der Schweiz haben wir eine umfassende Datenschutzgesetzgebung, zudem unterliegen wir den Richtlinien der Finanzmarktaufsicht. Was die Compliance-Anforderungen anbelangt, geben uns die Reports aus DatAdvantage weitere wichtige Hinweise, die wir natürlich auch den Data Ownern zugänglich machen werden.“

Die Zugriffsaktivitäten im Blick zu haben ist entscheidend um eine ganze Reihe von verbreiteten IT Problemen zu lösen und nicht in Anspruch genommene Berechtigungen zu identifizieren und zurücknehmen. Automatisierte Prozesse analysieren die Zugriffsaktivitäten und identifizieren gleichzeitig die Benutzer, die über zu umfassende Zugriffsrechte verfügen.

Michel Küng abschließend: „Mit Varonis verfügen wir über eine umfassende Management-Lösung für unsere Fileserver. Sie deckt sämtliche der von uns benötigten Funktionalitäten ab und kommt ohne Schnittstellen zu weiteren Systemen aus. Und letztendlich: jede Entscheidung, die für ein Unternehmen wie das unsrige besonders viel Tragweite hat, ist auch „peoples business“. Das persönliche und fachliche Engagement von Cyril Simonnet, David Lin und Patrick van der Veen von Varonis war ein klar differenzierender Faktor.“

Es gibt noch einige Details innerhalb der Varonis-Lösung, die für die Helvetia besonders interessant sind, beispielsweise die Option veraltete und nicht mehr benutzte Daten zu identifizieren. Nutzerstatistiken zeigen, dass schon 14 Tage nachdem ein User mit bestimmten Daten gearbeitet hat, auf diese Daten nicht mehr zugegriffen wird. Auch bei der Helvetia hatte sich bei einem ersten Check der historischen Daten ergeben, dass ein grosser Teil nicht aktiv benutzt wird.

„Daneben ist sicheres Filesharing ein großes Thema. Das haben wir mit Varonis für das dritte und vierte Quartal in diesem Jahr auf der Agenda. Jetzt stehen erst ein Mal noch die Schulung der ermittelten Data Owner und die Information unserer Enduser an.“

BUSINESS BENEFITS

LANGFRISTIG KONSOLIDIERTE BERECHTIGUNGEN – KONTROLLE, RISIKOMANAGEMENT, COMPLIANCE

Der Grundgedanke eines sicheren Umgangs mit Daten und Dateien ist der, dass ausschließlich die richtigen Benutzer Zugriff auf die Informationen haben, die sie brauchen, um ihre täglichen Aufgaben und Aktivitäten zu bewältigen – und nur auf diese Informationen. Und, dass diese Zugriffsaktivitäten nachvollziehbar sind. Bei geschätzten 5 Terabyte an Daten in 960.000 Ordnern und 3.200 Nutzungsberechtigen, die diese Daten verwenden, ist das weder manuell noch mit selbst entwickelten Tools zu bewerkstelligen. Mit Hilfe von DatAdvantage mit DataPrivilege können Berechtigungen über eine zentrale Oberfläche ermittelt, zugewiesen, entzogen und analysiert werden, ohne laufende Prozesse zu beeinträchtigen.

ZUGRIFFSAKTIVITÄTEN UND EREIGNISSE TRANSPARENT NACHVOLLZIEHEN

Die Zugriffsaktivitäten im Blick zu haben ist entscheidend um eine ganze Reihe von verbreiteten IT Problemen zu lösen und nicht in Anspruch genommene Berechtigungen zu identifizieren und zurücknehmen. Automatisierte Prozesse analysieren die Zugriffsaktivitäten und identifizieren gleichzeitig die Benutzer, die über zu umfassende Zugriffsrechte verfügen oder diese potenziell missbrauchen könnten. Das trägt aktiv zur IT-Sicherheit bei und garantiert Revisionssicherheit.

DATENKLASSIFIKATION & DATENNUTZUNG

Identifizieren von Daten, die nicht mehr genutzt werden, um potenzielle Risiken und Speicherkosten zu senken.

DATA GOVERNANCE – ENTSCHEIDUNGSHILFEN UND REPORTS FÜR DATA OWNER

Die aktuelle Lösung erlaubt ein effizientes Datenmanagement sowie das Nachvollziehen sämtlicher Zugriffsaktivitäten und Ereignisse. Das Reporting bietet wertvolle Analyse- und Prognosedaten, um sowohl die aktuelle Lage besser einschätzen als auch sich auf potenzielle Sicherheitsbedrohungen vorbereiten zu können.

ÜBER VARONIS

Varonis ist einer der führenden Hersteller von Data-Governance- und Data-Retention-Lösungen für unstrukturierte Daten. Diese nutzergenerierten Daten sind besonders sensibel und gehören zu der am schnellsten wachsenden Kategorie digitaler Informationen. Die Lösungen von Varonis basieren auf einer patentierten Technologie sowie einer hochpräzisen Analyse-Engine und bieten Organisationen einen umfassenden Überblick und vollständige Kontrolle über ihre Daten. So wird sichergestellt, dass nur die richtigen Benutzer jederzeit von allen Geräten aus auf die richtigen Daten zugreifen können sowie jegliche Nutzung der Daten überwacht und Missbrauch sofort gemeldet wird. Varonis macht die digitale Zusammenarbeit sicher, einfach und effizient und ermöglicht den Nutzern eine flexible Arbeitsweise. So können sie Inhalte erstellen und mit anderen berechtigten Nutzern austauschen. Unternehmen können sicher sein, dass ihre wertvollen Inhalte geschützt und effizient verwaltet werden.

Varonis wurde auf FastCompany.com zu einem der „Fast 50 Reader Favorites“ gewählt und mit dem Innovation Award, dem Product or Service of the Year Award sowie dem Best Network Security Award des SC Magazine ausgezeichnet. Das Unternehmen mit Hauptsitz in New York unterhält Niederlassungen in Europa und Asien und hat weltweit bereits mehr als 5.000 Lösungen implementiert.

Kostenlose 30-Tage-Testversion:

BEREITS STUNDEN NACH DER INSTALLATION

Können Sie direkt ein Audit Ihrer Berechtigungen durchführen: Datei- und Ordnerzugriffsberechtigungen und wie diese auf spezifische User und Gruppen verteilt sind. Sie können sogar Reports erstellen.

BEREITS EINEN TAG NACH DER INSTALLATION

Beginnt Varonis DatAdvantage Ihnen zu zeigen, welche Nutzer auf die Daten zugreifen und wie.

BEREITS 3 WOCHEN NACH DER INSTALLATION

Gibt Varonis DatAdvantage schon hochzuverlässige Empfehlungen, wie Sie den Zugriff auf Dateien und Ordner auf diejenigen User beschränken können, die ihn für ihre Arbeit auch benötigen.

DEUTSCHLAND, ÖSTERREICH UND SCHWEIZ

Varonis Deutschland GmbH, Welserstrasse 88, 90489 Nürnberg **T** +49(0) 911 8937 1111 **E** sales-germany@varonis.com **W** sites.varonis.com/de