VARONIS

WEISSBUCH

DSGVO-Compliance mit Varonis

Inhalt

Übersicht

Am 25.Mai 2018 wird die EU-Datenschutz-Grundverordnung (DSGVO) endlich in Kraft treten. Sie stellt die größte Veränderung des Datensicherheits- und Datenschutzrechts in der EU in über 20 Jahren dar. Die DSGVO baut auf die vorhandene Datenschutzrichtlinie auf und erweitert die bisherigen Bestimmungen in Bezug auf Datensicherheit und Datenschutz. Dabei führt sie eine Reihe bedeutender neue Anforderungen ein, wie z. B. die 72-Stunden-Frist für die Meldung von Datenschutzverletzungen und obligatorische Strafzahlungen.

Die DSGVO liefert kein vollständig neues Modell für den Datenschutz, sondern setzt auf die Ideen des Datenschutzes durch Technikgestaltung und andere Prinzipien des Datenschutzes. Allgemein formuliert könnte man sagen, dass die DSGVO nur vorhandene Praktiken des IT- und Datenschutzbetriebs zum Gesetz macht. Tatsächlich wird es die DSGVO (siehe § 40) den Unternehmen (bzw. den Datenverantwortlichen, in EU-Terminologie) ermöglichen, die Einhaltung der DSGVO durch Konformität mit vorhandenen Standards wie z. B. ISO 27001 oder PCI-DSS nachzuweisen.

Gibt es einen Ansatz für Datensicherheit, der viele unterschiedliche Standards und Gesetze einschließlich der DSGVO abdeckt und die Basis des Datenschutzprogramms in Ihrem Unternehmen bilden könnte?

Experten für Datensicherheit teilen Datenstandards im Allgemeinen in größere Kategorien ein (siehe dazu beispielsweise das CIS Framework von NIST). Hier sind drei, die üblicherweise auf den entsprechenden Listen auftauchen.

1. **Erkennen** – Identifizieren oder Lokalisieren von Risiken und Sicherheitslücken durch die Analyse von Dateisystemen, Verzeichnisdiensten, Kontoaktivitäten und Benutzerverhalten. Entwickeln der Kenntnisse im Unternehmen über Systeme, Ressourcen, Daten und Kompetenzen zum Handhaben von Cybersicherheitsrisiken

2. **Verhindern/Schützen** – Beschränken von potenziellen Datenschutzverletzungen in der Zukunft durch Sperren sensibler und veralteter Daten, Reduzieren allgemeiner und globaler Zugriffsberechtigungen und Vereinfachen der Berechtigungsstruktur.

3. **Pflegen** – Aufrechterhalten des sicheren Zustands durch Automatisieren der Genehmigungsabläufe, regelmäßige Anspruchsprüfungen und die Rückhaltung und Löschung von Daten. Überwachen ungewöhnlichen Benutzer- und Systemverhaltens.

Natürlich ist die DSGVO kein ausführlicher Standard für Daten-Compliance mit Hunderten von Unterkontrollen. Stattdessen sind in ihm die Anforderungen in Form von Artikeln aufgeführt, in denen allgemeine zu erreichende Ziele dargestellt werden, aber keine Anleitung, wie sie zu erreichen sind. Genauere Informationen über die DSGVO können Sie in unseren Whitepaper Die EU-Datenschutz-Grundverordnung: Neue Regeln für Datenschutz in der EU nachlesen.

Mit diesem Kategorisierungsschema haben wir nun eine Formel für die Strukturierung der wichtigsten DSGVO-Anforderungen und einen Angriffsplan:

	Artikel DSGVO	Varonis Produkt(e)
Erkennen	Sicherheit der Verarbeitung (Artikel 32)	DatAdvantage GDPR Patterns
	Datenschutz-Folgenabschätzung (Artikel 35)	
Schützen	Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Artikel 25)	DatAdvantage DataPrivilege Data Transport Engine DatAnswers
	Das Recht auf Löschen und „Vergessenwerden" (Artikel 17)	
	Verzeichnis von Verarbeitungstätigkeiten (Artikel 30)	
Pflegen	Meldung einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Artikel 33)	DatAlert
	Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person (Artikel 34)	

Zusammenfassend lässt sich der dreistufige Plan zur Erfüllung des DSGVO so darstellen: Identifizierung gefährdeter Ressourcen, Schutz dieser Ressourcen durch die Pflege angemessener Berechtigungen und Einsatz anderer Prinzipien des Datenschutzes durch Technikgestaltung, und schließlich Überwachung dieser Ressourcen auf Gefahren.

Es gibt tatsächlich einen vierten Schritt, nämlich die Erkenntnisse aus der Erkennungs-/Überwachungsphase wieder in den ersten Schritt zurückführen. Mit anderen Worten, Sie nehmen eine Feinabstimmung der ersten drei Schritte auf der Grundlage Ihrer Erkenntnisse aus der Überwachung auf Bedrohungen oder andere Schwachstellen vor.

Bei Varonis wählen wir einen datenzentrierten Ansatz im Hinblick auf Datensicherheit. Mit unseren Produkten, insbesondere DatAdvantage, DataPrivilege, DatAlert und unserer Data Classification Engine, können wir in den Teilen des IT-Systemen, in denen Sicherheitsvorrichtungen am sinnvollsten einzusetzen sind, Daten schützen und das Risiko von Datendiebstahl reduzieren oder sogar eliminieren – und zwar nicht am Perimeter, wo der Schutz umgangen werden kann, sondern an den Daten selbst.

Lassen Sie uns den Plan nun genauer betrachten.

Grundlegende Erkennung

Um Ihre potenziellen Schwachstellen und Risiken zu verstehen, ist es sinnvoll, eine Inventarisierung Ihres Systems durchzuführen und nach bestimmten Ressourcen und Risiken zu suchen. Für Varonis sind Benutzer, Gruppen und Ordner die grundlegenden Bestandteile und das Ausgangsmaterial aller Risikoberichte.

Als ersten Schritt in Richtung DSGVO-Konformität sollten Sie grundlegende Informationen zu Dateisystem-Ressourcen und Konten überprüfen. Dabei können Ihnen die folgenden, mit DatAdvantage generierten Berichte eine große Hilfe sein.

Im DatAdvantage 4G-Bericht von Varonis können Sicherheitsfachkräfte schnell die Ordner mit personenbezogenen Daten gemäß DSGVO erkennen, die häufig quer über das Dateisystem des Unternehmen verstreut liegen. Das ist ein großartiger Einstig in die Verminderung von Risiken.

Hinter den Kulissen hat die Varonis Data Classification Engine bereits die Dateien mit Spezialfiltern gescannt, die für personenbezogene Daten wie Telefonnummern und Kontonummern typische Muster identifizieren können, und die Dateien auf Grundlage der Trefferanzahl bewertet.

Classification Results (Selected Rules)	Hit Count	Risk%	Files with Hits	Scan Priority
GDPR UK (258/258), **GDPR Belgium** (120/120), **GDPR Poland** (120/120), **American Express** (122/122), **DE Personal Data Protection** (120/120), **MasterCard** (175/175), **PCI Data Security Standards** (PCI-DSS) (743/743), **DE Landline Phone Numbers** (120/120), **Visa** (322/322)	2100	5.69	6	252
GDPR UK (134/134), **GDPR Belgium** (100/100), **GDPR Poland** (100/100), **American Express** (102/102), **DE Personal Data Protection** (100/100), **MasterCard** (102/102), **PCI Data Security Standards** (PCI-DSS) (446/446), **DE Landline Phone Numbers** (100/100), **Visa** (322/322)	1394	3.77	2	254

▲ *DatAdvantage 4g zeigt die Ergebnisse der Datenklassifizierung*

Als Hilfsmittel speziell für die identifizierung von personenbezogene Daten gemäß DSGVO hat Varonis die GDPR Patterns eingeführt. Mit ihnen können Unternehmen personenbezogene Daten laut DSGVO erkennen: von Ausweisnummern über IBAN oder Blutgruppe bis hin zu Kreditkartendaten. Das bedeutet, dass Sie unterschiedliche Berichte über die laut DSGVO relevanten personenbezogenen Daten erstellen können, einschließlich Berechtigungen, uneingeschränktem Zugriff und Angaben zum letzten Zugriff (veraltete Daten).

Welche von der DSGVO betroffenen Daten werden nicht mehr benötigt?

Der Bericht 4f über Ordner enthält Zugriffspfade, Größe, Anzahl der Unterordner und den Freigabepfad. Indem man das letzte Zugriffsdatum als Suchkriterium wählt, kann man außerdem eine Liste der selten genutzten Ordner erstellen – also von „veralteten Daten“. Wie wir im nächsten Abschnitt besprechen, können diese Informationen beim Minimieren von Datensicherheitsrisiken hilfreich sein.

Wo liegen laut DSGVO relevante Daten offen?

Auch der Bericht 4b ist sehr nützlich. Er zeugt die Berechtigungen für einen bestimmten Ordner an, optional aufgeschlüsselt nach Gruppen der ACLs. Außerdem liefert er Empfehlungen im Hinblick auf Berechtigungen zu Gruppenmitgliedschaften. Wenn die Zugriffskontrollen für einen bekannten kritischen Datensatz schnell überprüft und angepasst werden sollen, ist der Bericht 4b für diesen Zweck am besten geeignet.

Die vorstehend besprochenen Berichte enthalten einige zentrale Identifikationsinformationen, die in der „Schutz“-Phase für Gegenmaßnahmen verwendet werden können. Zur Erinnerung: Mit der DSGVO werden übliche Vorgehensweisen der IT-Sicherheit zum Gesetz gemacht: hier das „Implementieren angemessener Maßnahmen auf technischer und organisationeller Ebene“. Die Berichte von DatAdvantage über offen zugängliche Daten, wahrheitsgetreue Listen mit Gruppenmitgliedschaften und veraltete Daten sowie Benutzerkonten werden der IT-Gruppe dabei behilflich sein, diese Maßnahmen umzusetzen.

Identifizieren und Risiken

Während die Basisberichte einen guten Ausgangspunkt bieten, müssen IT-Sicherheitsmitarbeiter tiefer in das Dateisystem eindringen, um sensible oder kritische Daten zu identifizieren, die eine Risikoquelle darstellen können.

Im Allgemeinen suchen sie nach persönlich identifizierbaren Daten (PII) oder personenbezogenen Daten, wie sie in der DSGVO genannt werden, wie E-Mail-Adressen, Telefonnummern, Führerscheinnummern und Ausweisnummern.

Wie uns die großen Datenschutzverletzungen der letzten Jahre gezeigt haben, sind schlecht geschützte Ordner – Ordner oder Verzeichnisse mit unnötig großzügigen Berechtigungen – der Ort, an dem Hacker aktiv werden. Sobald sie eingedrungen sind, nutzen Hacker einfach die Zugriffsberechtigungen des Kontos, das sie übernommen haben.

Der DatAdvantage 4c-Bericht ist der erste Bericht, der es Ihnen ermöglicht, global zugängliche DSGVO-relevante Daten innerhalb bestimmter Dateien aufzuspüren.

Access Path	User/Group	Current Permissions	Total Hit Count (Inc. subfolders)	Classification Results
rojects11.txt (1)	Abstract\ Everyone	FMRWX	10	**GDPR UK** (2/2), **MasterCard** (2/2), **DE Personal Data Protection** (5/5), **Visa** (1/1)
C:\share\84\ProjectData.txt (1)	Abstract\ Everyone	FMRWX	113	**GDPR Belgium** (16/16), **GDPR Poland** (16/16), **DE Personal Data Protection** (17/17), **Mastercard** (5/5), **PCI Data Security Standards (PCI-DSS)** (16/16), **DE Landine Phone Numbers** (16/16), **Visa** (11/11)

▲ *Abbildung 3 Der Bericht 4a von DatAdvantage zeigt Dateien mit sensiblen Daten, die global zugänglich sind.*

Personenbezogene Daten gemäß DSGVO in Dateien, die für jeden im Unternehmen zugreifbar sind, stellen ein erhebliches Risiko dar. Der Bericht 4a von DatAdvantage zeigt Ihnen diese Dateien. Außerdem kann der Bericht 4a so konfiguriert werden, dass er nur Ordner mit global zugänglichen personenbezogene Daten gemäß DSGVO anzeigt.

Er kann anstelle des Berichtes 4g (siehe oben) verwendet werden, um einen fokussierteren ersten Überblick über Ihre Umgebung zu gewinnen. Übrigens: Je vertrauter Sie mit den flexiblen Filteroptionen der DatAdantage-Berichte werden, desto wahrscheinlicher ist es, dass Sie einen eigenen Ansatz für das DSGVO-Sicherheitsprogramm Ihres Unternehmens finden.

Wir kennen jetzt die Ordner, die potenzielle Quellen für Datenschutzrisiken sind.

Was wollen wir noch erkennen?

Ein guter Ausgangspunkt wären die Benutzer, die auf diesen Ordner zugegriffen haben.

Es gibt einige Methoden, wie Sie das mit DatAdvantage tun können, aber wir wollen hier einfach mit den Zugriffs-Auditprotokollen aller Dateiereignisse auf einem Server in Rohform arbeiten, die uns im Bericht 2a zur Verfügung stehen. Durch Hinzufügen eines Filters für den Zugriffspfad können Sie die Ergebnisse auf einen bestimmten ordner einengen.

Date	User Name	File Server	Access Path	Event Type	Event Count
					46806
7/6/2015	corp.local\Alice Tanner	Corpfs02b	C:\Share\legal\Corporate\Finance	All event types	9
7/10/2015	corp.local\Alice Tanner	Corpfs02b	C:\Share\legal\Corporate\Finance	All event types	35
7/2/2015	corp.local\Alice Tanner	Corpfs02b	C:\Share\legal\Corporate\Finance	All event types	20
7/10/2015	corp.local\Alice Tanner	Corpfs02b	C:\Share\legal\Corporate\Distrobution Agreements\ DISTRIB (TEXIM EUROPE) V1 REVI.txt	All event types	1
1/7/2016	corp.local\Alice Tanner	Corpfs02b	C:\Share\legal\Corporate\CLA USES	File opened	1

▲ *Abbildung 4 Der Bericht 2a von DatAdvantage 2a zeigt Ordner mit personenbezogenen Daten gemäß DSGVO.*

Veraltete Benutzerkonten sind ein weiteres Szenario mit Risikopotenzial, das häufig übersehen wird. Letztlich werden häufig Benutzerkonten nicht deaktiviert oder gelöscht, wenn ein Mitarbeiter das Unternehmen verlässt oder ein zeitlich begrenzter Auftrag eines externen Dienstleisters beendet ist.

Für den verärgerten Mitarbeiter ist es nicht ungewöhnlich, dass er als ehemaliger Insider auch nach seinem Ausscheiden aus dem Unternehmen noch Zugang zu seinem Konto hat. Häufig verschaffen sich auch Hacker Zugang über ein nicht mehr genutztes Konto eines externen Dienstleisters und nutzen es dann, um zum tatsächlichen Angriffsziel zu springen. In der Schutzphase behandeln wir, wie Varonis Sie dabei unterstützt, diese Konten schnell zu deaktivieren.

Ein vollständiges Risikobeurteilungsprogramm würde außerdem die Identifizierung externer Gefahren – neuer Malware und neuer Hacking-Methoden – beinhalten. Das ist eine Funktion, die mit der Identifzierung der Datenbestände getrennt ist. Mit diesen neuen Informationen über tatsächlich existierende Gefahren könnten Sie Ihre anfänglich eingestellten Risikostufen anpassen und danach Ihre Strategie neu ausrichten. Das sollte auf laufender Basis erfolgen, weil im Cyberspace das Katz-und-Maus-Spiel mit den Hackern niemals endet.

Verhindern

In der zweiten Phase der DSVGO-Methodologie von Varonis werden Berechtigungen neu strukturiert, zu frei zugängliche personenbezogene Datenbestände gesperrt oder reduziert und Daten-Eigentümer identifiziert, um sicherzustellen, dass wir angemessene vorbeugende Kontrollmechanismen einführen. Dadurch werden Bereiche mit hohem Gefährdungsgrad beseitigt, Angriffsflächen für potenzielle Angriffe verkleinert und die Umgebung vereinfacht. Außerdem beginnen wir damit, Stakeholder außerhalb der IT-Sicherheitsabteilung in die Prozesse einzubeziehen.

In dieser Phase setzen Sie ein Schlüsselprinzip der DSGVO um: die Minimierung. Sie suchen mithilfe der Datei- und Kontoinformationen nach Wegen, um die Anzahl der Personen, die auf personenbezogene Daten zugreifen können, und die Menge der sensiblen Daten selbst zu reduzieren.

Wir wollen uns anschauen, wie sich diese Aufgabe in der Phase „Verhindern“ bewerkstelligen lässt.

Zu den kritischen Kontrollen in diesem Bereich gehört die Einschränkung des Zugriffs auf autorisierte Benutzer. Das ist leichter gesagt als getan, aber die Grundlagenarbeit haben wir im Voranstehenden bereits geleistet.

Als Leitprinzipien ziehen wir das Prinzip der notwendigsten Berechtigung und rollenbasierte Zugriffskontrollen heran. Kurz formuliert: Wir geben nur den Benutzern Zugriff auf die Daten, die sie zum Ausführen ihrer Aufgaben bzw. zur Erfüllung ihrer Rollen benötigen.

Da wir hier einen Punkt erreicht haben, an dem wir wirklich aktiv eingreifen, müssen wir innerhalb von DatAdvantage aus dem Berichtsbereich in den Überprüfungsbereich wechseln.

DatAdvantage unterstützt uns mit grafischen Darstellungen bei der Identifizierung der Dateneigentümer.

Wenn Sie sich eine detailliertere Darstellung wünschen, die über die Personen, die auf einen Ordner zugegriffen haben, hinausgeht, können Sie sich die genauen Zugriffsstatistiken der aktivsten Benutzer auf der Registerkarte Statistik in DatAdvantage anzeigen lassen.

Das ist sehr hilfreich dabei, sich ein Bild der Personen zu verschaffen, die tatsächlich mit den Ordnern arbeiten. Das Ziel ist letztlich, die wahren Benutzer zu finden und überflüssige Gruppen und Benutzer zu entfernen, die möglicherweise in Einzelfällen, die nicht zu ihren regulären Aufgaben gehören, zugreifen mussten.

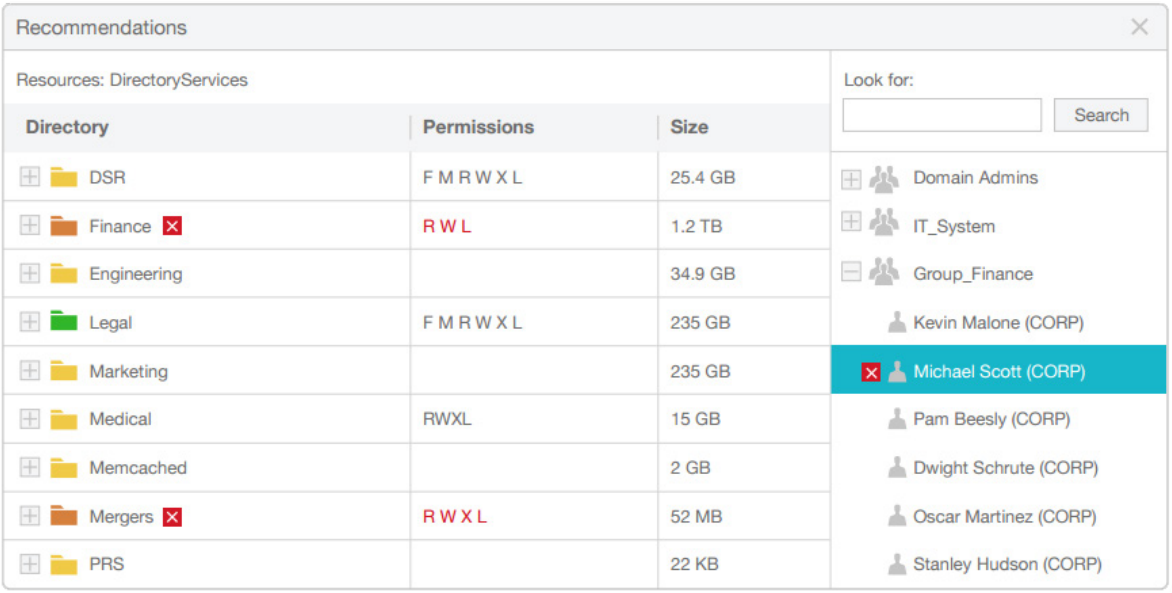
Der springende Punkt ist, den Eigentümer des Ordners festzulegen – die Person, die über echte Kenntnisse und Informationen darüber verfügt, welchem Zweck dieser Ordner tatsächlich dient. Das kann für die IT-Abteilung mit einer gewissen Laufarbeit in Form von Gesprächen mit Benutzern auf der Grundlage der DatAdvantage-Statistiken verbunden sein, um die tatsächliche Weisungshierarchie herauszuarbeiten.

Sobald Sie mit DatAdvantage Eigentümer für die Ordner festgelegt haben, können diese besser informierten Benutzer unabhängig darüber entscheiden, wer Zugriff haben sollte und welche Zugriffsberechtigungen widerrufen werden sollten. Die Ordner-Eigentümer erhalten außerdem automatisch Berichte von DatAdvantage, die sie bei zukünftigen Entscheidungen über Zugriffsberechtigungen unterstützen.

Bevor wir uns der nächsten Phase zuwenden, sollte ein Punkt unbedingt erwähnt werden. IT ist lange für die Bereitstellung von Zugriffsberechtigungen zuständig gewesen, ohne den geschäftlichen Zweck wirklich zu kennen. Varonis DatAdvantage unterstützt die IT-Abteilung beim Auffinden dieser Eigentümer und diese wiederum bei der Minimierung oder Einschränkung von Zugriffsberechtigungen und danach bei der formellen Berechtigungsverwaltung.

Eine weitere Hilfestellung von DatAdvantage für Daten-Eigentümer ist die automatische Empfehlungs-Engine. Daten-Eigentümer finden diese Empfehlungen häufig nützlich, weil sie mit ihnen leicht Benutzer erkennen können, deren Rollen sich geändert haben und deshalb keinen Zugriff mehr benötigen usw. Der Bericht 4b aus dem letzten Abschnitt wäre hier hilfreich, weil in ihm die ACL-Empfehlungen aufgeführt werden.

Auch die Registerkarte Arbeitsbereich in DatAdvantage enthält ähnliche Informationen.



▲ *DatAdvantage 4g zeigt die Ergebnisse der Datenklassifizierung*

Wie auch immer, sobald der Eigentümer durch das Einschränken und Entfernen unnötiger Benutzer und Gruppen für Ordnung gesorgt hat, sollten Sie einen Prozess für das Berechtigungsmanagement einrichten.

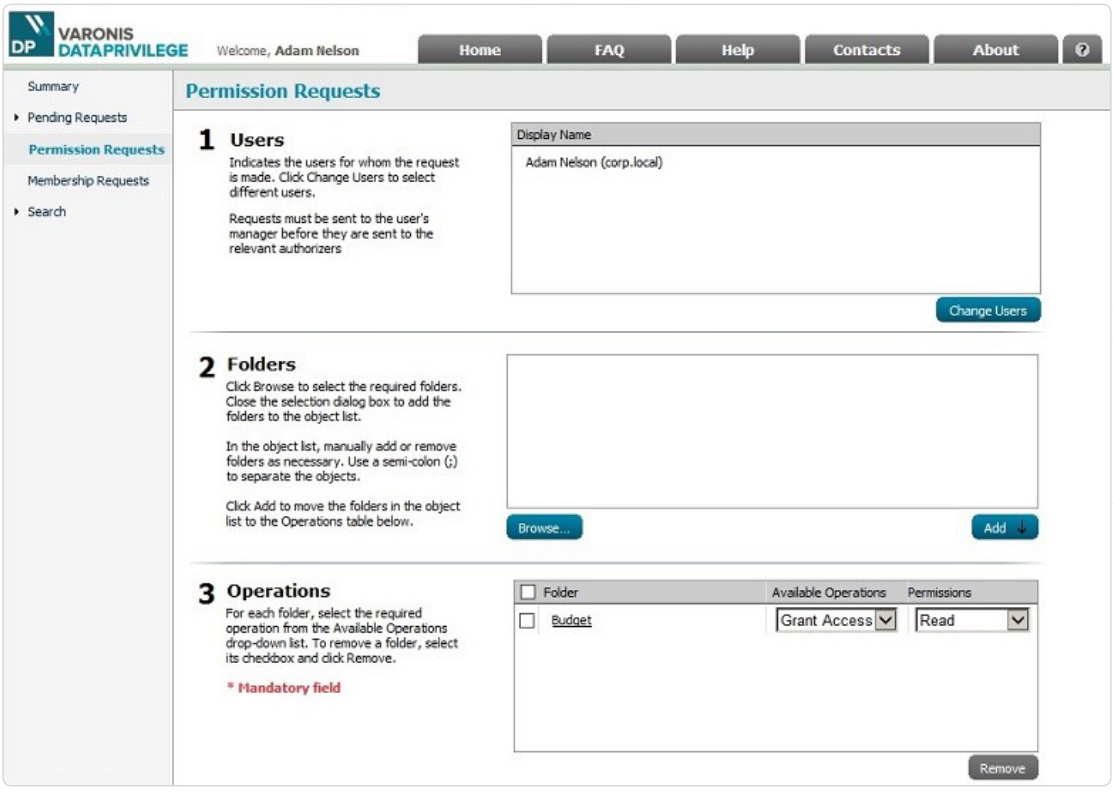
Datenschutzstandards und -gesetze wie die DSGVO erkennen an, wie wichtig es ist, Sicherheitsrichtlinien und -verfahren als Bestandteil eines fortlaufenden Programms durchzusetzen – also nicht nur einmal im Jahr durch den Verantwortlichen.

Auch hier kann Varonis eine wichtige Rolle übernehmen.

Pflege des Prinzips der notwendigen Berechtigung

Wie beantragen normale Benutzer, die aufgrund ihrer Rolle auf einen verwalteten Ordner zugreifen müssen, die entsprechende Berechtigung beim Veranwortlichen?

An dieser Stelle kommt Varonis DataPrivilege ins Spiel. Normale Benutzer beantragen den Zugriff auf einen verwalteten Ordner über DataPrivilege, und DataPrivilege steuert danach den Verlauf des Workflows.



Der für den Ordner Verantwortliche hat eine Parallelschnittstelle, über die er diese Anträge erhält und Berechtigungen zuteilen oder widerrufen kann. Dabei besteht das Ziel darin, den Workflow für die Aktivierung von Zugriffsberechtigungen automatisch auf die Personen einzuschränken, die wirklich zugreifen müssen.

Eine andere Methode zur Pflege des Prinzips der notwendigsten Berechtigung ist die Deaktivierung von veralteten oder inaktiven Konten. Sie stellen ein potenzielles Sicherheitsrisiko dar. Diese Konten können mit DatAdvantage direkt über die Online-Bedienoberfläche deaktiviert werden, was den zusätzlichen Schritt einspart, extra einen Verzeichnisdienst wie z. B. Active Directory aufrufen zu müssen.

Minimieren sensibler Daten

Minimierung ist in Datenschutzstandards und -gesetzen ein wichtiges Thema. Diese Ideen werden am besten durch die Grundsätze des Datenschutzes durch Technikgestaltung illustriert, die allgemeingültige gute Ratschläge für den Datenschutz enthalten: Minimieren Sie die sensiblen Daten, die Sie sammeln, minimieren Sie die Gruppe, die Einblick in sie hat, und minimieren Sie die Zeitspanne, über die diese Daten aufbewahrt werden.

In der DSGVO werden diese Ideen direkt im Artikel „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ (Artikel 25) aufgeführt.

Wir haben bereits besprochen, wie DatAdvantage bei der Minimierung des Personenkreises mit Zugriffsmöglichkeit helfen kann. Ein weiteres Prinzip des Datenschutzes durch Technikgestaltung ist, Risiken durch das Löschen oder Archivieren unnötiger oder veralteter sensibler Daten in Dateien zu minimieren.

Das macht sehr viel Sinn. Veraltete personenbezogene Daten gemäß DSGVO können beispielsweise Verbraucher-IDs sein, die in kurzfristigen Marketingkampagnen gesammelt wurde und nun in kaum genutzten Datentabellen oder Management-Präsentationen vorliegen.

Ihr Unternehmen benötigt sie wahrscheinlich nicht mehr, aber es handelt sich bei ihnen genau um die Art von verkaufsfähigen Daten, die Hacker für Hacker besonders interessant sind.

DatAdvantage kann Dateidaten finden und identifizieren, die über ein bestimmtes Datum hinaus nicht mehr genutt wurden. Lässt sich der Bericht 4f von DatAdvantage (aus dem vorstehenden Abschnitt) so anpassen, dass er veraltete Daten findet, die gleichzeitig personenbezogene Daten laut DSGVO sind?

Ja.

Sie müssen den Filter „Hit Count“ hinzufügen und die Anzahl der Treffer für sensible Daten auf den passenden Wert setzen.

Der nächste Schritt besteht darin, die Data Transport Engine (DTE) von DatAdvantage (im Menü Tools verfügbar) einzusetzen. Mit der DTE können Sie eine Regel erstellen, mit der nach Dateien für die Archivierung oder, im Bedarfsfall, zum Löschen gesucht wird.

Die Suchkriterien der Regel sind identisch mit den Filtern, die im vorstehenden Abschnitt zum Generieren der Berichte über sensible Daten verwendet wurden. Die Regel erledigt dann die aufwendige Arbeit, die veralteten sensiblen Daten zu erkennen und zu entfernen.

Weil Sie die Regel auch speichern können, kann sie jederzeit erneut ausgeführt werden, um die zeitlichen Beschränkungen der Aufbewahrung durchzusetzen. Noch besser: Die DTE kann die Regel regelmäßig automatisch ausführen, so dass Sie sich nie wieder Gedanken über veraltete personenbezogene Daten mit Relevanz für die DSGVO in Ihrem System machen müssen.

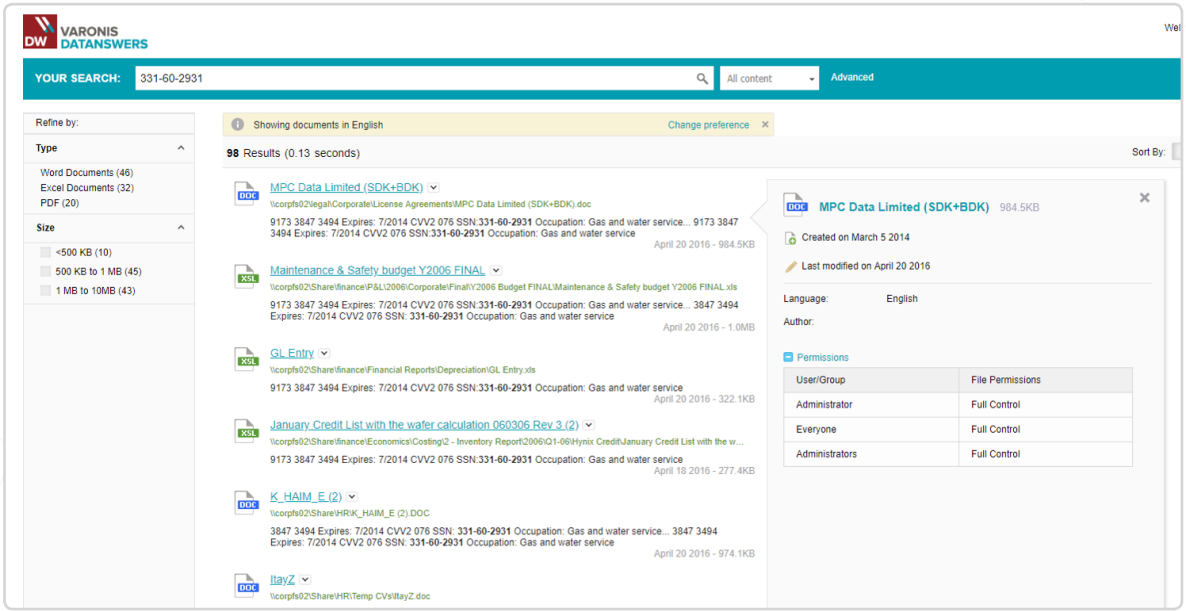
Das Recht auf Vergessenwerden

Varonis kann auch bei der Erfüllung einer anderen Anforderung der DSGVO helfen: dem „Recht auf Löschung und Vergessenwerden“ (Artikel 17).

Der DSGVO zufolge haben die Verbraucher das Recht, die Löschung der sie betreffenden personenbezogenen Daten zu verlangen. Diese Anforderung umfasst nicht nur die Entfernung personenbezogener Daten aus strukturierten Datenbanken sondern auch aus Dateisystemen.

Sie könnten zwar neue Klassifizierungsregeln hinzufügen, um einen bestimmten Kunden zu finden – z. B. mit Hilfe von Suchkriterien für Namen oder Kontonummern – und die Löschung zu beantragen, aber Varonis DatAnswers bietet einen einfacheren Weg, um dem Recht auf Löschung nachzukommen. DatAnswers ist unsere intelligente Suchmaschine zum Scannen von Dateien.

Genau wie Sie Suchwörter in Google eingeben würden, können mit DatAnswers die Dateien zu finden, in denen sich die personenbezigenen Daten eines Kunden befinden, der die Löschung beantragt. Und dann können Sie die Datei in die Quarantäne verschieben oder ihren Inhalt anpassen.



Überwachen

Es gibt keine fehlerfreien Datensicherheitsstrategien, weshalb Sie eine sekundäre Verteidigung auf der Grundlage von Erkennungs- und Überwachungskontrollen benötigen: Dabei beobachten Sie das System und suchen nach ungewöhnlichen Aktivitäten, die auf die Aktivität eines Hackers hindeuten.

Varonis DatAlert übernimmt eine einzigartige Rolle bei der Erkennung von Datenschutzverletzungen, weil die zugrunde liegende Sicherheitsplattform auf der Überwachung von Dateisystemaktivitäten basiert.

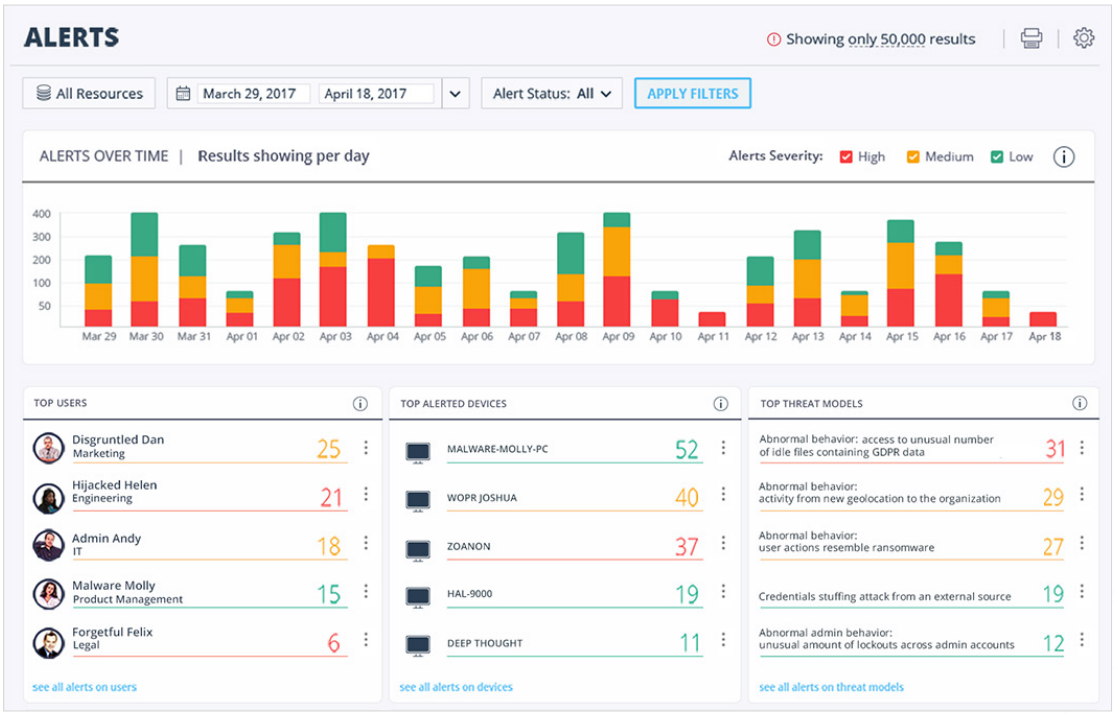
Mittlerweile weiß jeder (oder sollte wissen), dass Hacker mit Phishing- und Injektionsangriffen die Netzwerkverteidigung umgehen können, indem sie die Zugangsdaten bestehender Benutzer übernehmen, und dass Fully Undetectable Malware (FUD) auch der Erkennung durch Virenscanner entgehen kann.

Wie lässt sich also die neue Generation getarnter Angreifer erkennen?

Alle Angreifer *müssen* das Dateisystem benutzen, um Software zu laden, Dateien zu kopieren oder Verzeichnishierarchien zu durchsuchen, wenn sie nach sensiblen Daten suchen, um diese zu exfiltrieren. Wenn Sie die entsprechenden einzigartigen Dateiaktivitätsmuster erkennen können, dann können Sie diese auch stoppen, bevor die Daten entfernt oder exfiltriert werden, oder zumindest die Menge der zugänglichen Daten begrenzen.

Wir können hier nicht auf alle Funktionen von DatAlert eingehen. Aber da DatAlert über tiefen Einblick in alle Dateisysteminformationen und -ereignisse sowie in den Verlauf des Benutzerverhaltens verfügt, ist es besonders gut aufgestellt, um Aktivitäten außerhalb des normalen Aktivitätsbereiches eines Benutzerkontos zu erkennen.

Wir bezeichnen diese Vorgehensweise als Analysen des Nutzerverhaltens (User Behaviour Analytics, UBA), und DatAlert wird mit einem Bündel von UBA-Bedrohungsmodellen ausgeliefert. Sie können natürlich auch eigene Modelle hinzufügen, aber die fertig definierten Modelle sind schon extrem leistungsfähig. Mit ihnen können Sie Krypto-Intrusionen, Ransomware, ungewöhnliche Zugriffsaktivitäten auf sensiblen Daten, ungewöhnliche Zugriffsaktivitäten auf Dateien mit Anmeldeinformationen und zahlreiche andere Aktivitäten erkennen.



Ausgelöste Warnmeldungen können Sie über das DatAlert Dashboard verfolgen. IT-Mitarbeiter können dann entweder manuell eingreifen und reagieren oder automatisch ausgeführte Skripte einrichten – z. B. um Konten automatisch zu deaktivieren.

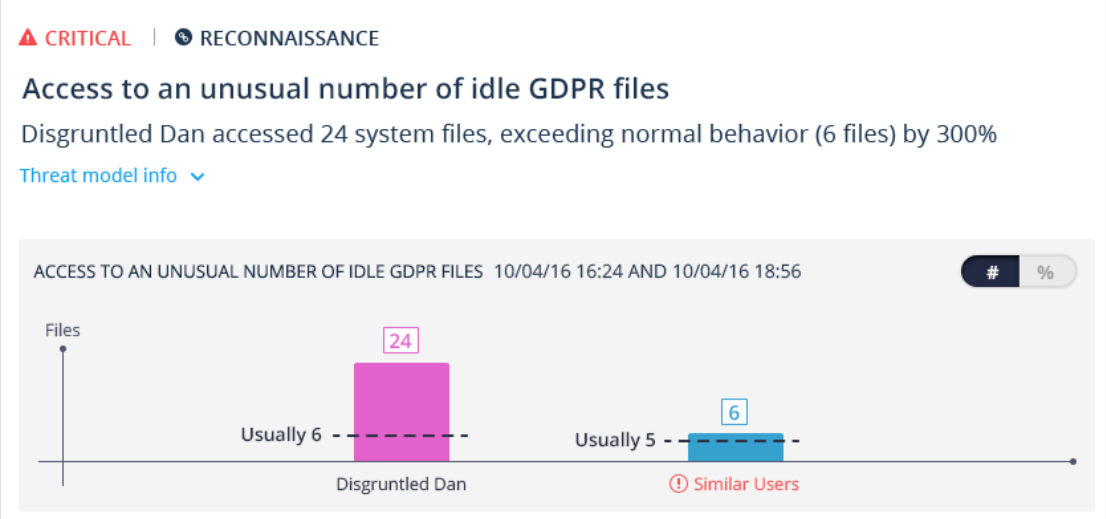
Die Pflicht zur Meldung von Datenschutzverletzungen gemäß DSGVO (Artikel 33, 34) sieht vor, dass die Aufsichtsbehörde über die Art der Verletzung, die Datenkategorien und die Anzahl der betroffenen Datensätze sowie über Maßnahmen zur Behebung des Verstoßes informiert werden muss.

DatAlert kann diese Informationen alle liefern und gleichzeitig die Sicherheitslücke durch Ausführung automatischer Skripte schließen.

Hier finden Sie einige Beispiele für die Bedrohungsmodelle, die zu Entdeckung und als Handlungsgrundlage dienen können:

Bedrohungsmodell	Beschreibung
Ungewöhnliches Verhalten: **Zugriff auf eine ungewöhnliche Anzahl ungenutzter DSGVO-Dateien**	Es wurde ein statistisch signifikanter Anstieg in der Anzahl der geöffneten DSGVO-Dateien durch den Benutzer im Vergleich zu seinem Verhaltensprofil entdeckt. Ungenutzte Dateien sind Dateien, die der Benutzer nicht erstellt oder im Rahmen seiner Zugriffe verändert hat, und auf die er vorher sehr lange nicht zugegriffen hat (wobei andere Benutzer allerdings erst kürzlich auf sie zugegriffen haben dürfen). Dieses Verhalten könnte darauf hinweisen, dass ein Angreifer nach Datenbeständen mit sensiblen Daten sucht, auf die er zugreifen kann, um diese Daten zu exfiltrieren.
Ungewöhnliches Verhalten: **Ungewöhnlich hohe Anzahl verweigerter Zugriffe auf DSGVO-Dateien**	Es wurde ein statistisch signifikanter Anstieg in der Anzahl der DSGVO-Dateien entdeckt, auf die ein Benutzer erfolglos zugreifen wollte. Dieses Verhalten könnte darauf hinweisen, dass ein Angreifer versucht, Zugriff auf unterschiedlichen Datenbestände zu erlangen, um Daten zu exfiltrieren.
Ungewöhnliches Verhalten: **Ungewöhnlich hohe Anzahl gelöschter oder geänderter DSGVO-Dateien**	Es wurde ein statistisch signifikanter Anstieg in der Anzahl der durch den Benutzer gelöschten oder geänderten DSGVO-Dateien im Vergleich zu seinem Verhaltensprofil entdeckt. Dieses Verhalten könnte darauf hinweisen, dass ein Angreifer versucht, kritische Datenbestände zu beschädigen oder zu zerstören, beispielsweise im Rahmen eines Denial-of-Service-Angriffs.
Ungewöhnliches Verhalten: **Zugriff auf untypische Ordner mit DSGVO-Daten**	Ein Dienstkonto hat auf Ordner mit DSGVO-Daten zugegriffen, auf die es zuvor noch nicht zugegriffen hat. Dienstkonten sollten wiederholt identische Aktionen durchführen. Eine Verhaltensänderung ist deshalb verdächtig. Angreifer können sich als Dienstkonto ausgeben und dessen Berechtigungen missbrauchen.

Damit Sie die in der DSGVO vorgesehene 72-Stunden-Frist zur Bereitstellung von Informationen für die Datenbehörden erfüllen können, lassen sich die Verhaltensmuster der Bedrohungserkennung von DatAlert so anpassen, dass sie sich ausschließlich auf personenbezogene Daten gemäß DSGVO konzentrieren. Sie können sich also einfach gesagt Benachrichtigungen über ungewöhnliche Zugriffsaktivitäten auf einen Ordner mit Telefon- oder Ausweisnummern anzeigen lassen.



▲ *Abbildung 9 DatAlert kann zum Auslösen von Benachrichtigen bei Bedrohungen, die personenbezogene Daten gemäß DSGVO betreffen, konfiguriert werden.*

Sonstige Aspekte

Sie sollten unbedingt daran denken, dass die DSGVO kein Datenschutzstandard ist. Sie bietet Leitlinien – die natürlich von den EU-Regulierungsbehörden durchgesetzt werden – zur Gewährleistung des Schutzes personenbezogener Daten.

Die DSGVO verlangt von Ihnen, dass Sie „geeignete technische und organisatorische Maßnahmen [ergreifen], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“ - siehe Sicherheit der Verarbeitung (Artikel 32). Die DSGVO verlangt von Ihnen auch die Einrichtung von Prozessen zur „regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen“.

Anders formuliert: Datenschutz ist eine Aufgabe, die fortlaufend durchgeführt werden muss. Wir haben in diesem White Paper dargelegt, wie die Software von Varonis Sie bei Ihrem mit der DSGVO konformen Datensicherheitsprogramm unterstützen kann. Wir sind nicht auf alle Fähigkeiten von Varonis eingegangen, und wenn Sie weitere Informationen wünschen, können Sie sich den operativen Plan von Varonis betrachten. Eine Kopie erhalten Sie von unseren Vertriebsmitarbeitern.

Viele große Unternehmen haben sich bisher wahrscheinlich auf vorhandene Datensicherheitsstandards wie PCI DSS oder ISO 27001 verlassen und bereits viele der in diesen Standards vorgesehenen detaillierten Sicherheitskontrollen implementiert.

Wenn das bei Ihnen der Fall ist, müssen Sie diese Kontrollen nun gezielter auf den Schutz personenbezogener Daten gemäß DSGVO fokussieren.

Das DSGVO bietet mit ihren genehmigten „Verhaltensregeln“ (siehe Artikel 40) einen Weg, um „Kredit“ für bereits bestehende Compliance zu erhalten.

Artikel 40 sieht vorm, dass Normenverbände ihre Sicherheitskontrollen, z. B. PCI DSS, dem European Data Protection Board (EDPB) zur Genehmigung vorlegen können. Wenn ein Unternehmen dann einer offiziell genehmigten „Verhaltensregel“ folgt, kann dies die Aufsichtsbehörde von der Einleitung weiterer Maßnahmen, einschließlich der Verhängung von Bußgeldern, abhalten, solange der Normenverband - zum Beispiel der PCI Security Standards Council - über einen eigenen Überwachungsmechanismus zur Überprüfung der Einhaltung seiner Standards verfügt.

Die DSGVO geht allerdings noch einen Schritt weiter. Sie hält auch einen Weg für eine Zertifizierung des Unternehmen – oder in der Terminologie der DSGVO: eines Verantwortliche – hinsichtlich seines Umgangs mit Daten offen.

Im Endeffekt sind die Aufsichtsbehörden (durch Artikel 40) befugt, den Betrieb eines Verantwortlichen als mit der DSGVO konform zu zertifizieren. Die EU-Aufsichtsbehörden können auch andere Normenverbände wie PCI oder ISO für die direkte Erteilung derartiger Zertifizierungen akkreditieren.

Die Zertifizierung läuft nach drei Jahren ab- danach muss das jeweilige Unternehmen seine Zertifizierung erneuern.

Diese Zertifizierungen erfolgen vollständig freiwillig. Sie werden jedoch offenkundig für viele Unternehmen sehr vorteilhaft sein. Die Absicht dieser Regelung besteht darin, die vorhandenen Datenschutzstandards der Privatwirtschaft zu nutzen und Unternehmen einen praxisorientierten Ansatz für ihre Konformität mit den technischen und administrativen Auflagen der DSGVO zu bieten.

Das EDPB wird voraussichtlich auch an Endverbraucher gerichtete Zertifizierungszeichen und -siegel und ein Register für zertifizierte Unternehmen entwickeln.

Für weitere Informationen über die DSGVO-Zertifizierung werden wir auf weitere Mitteilungen der Behörden warten müssen.

> Varonis ist eine fantastische Lösung.

Gartner peerinsights™

Vereinbaren Sie eine DSGVO-Bereitschaftsprüfung

Bewertung des Datenrisikos

Sie erhalten Ihr Risikoprofil, entdecken Sicherheitslücken und beheben echte Sicherheitsprobleme.

info.varonis.com/gdpr-risk-assessment-de

Live-Demo

Richten Sie Varonis in Ihrer eigenen Umgebung ein, um zu beobachten, wie Ransomware gestoppt und Ihre Daten geschützt werden.

varonis.com/demo-de