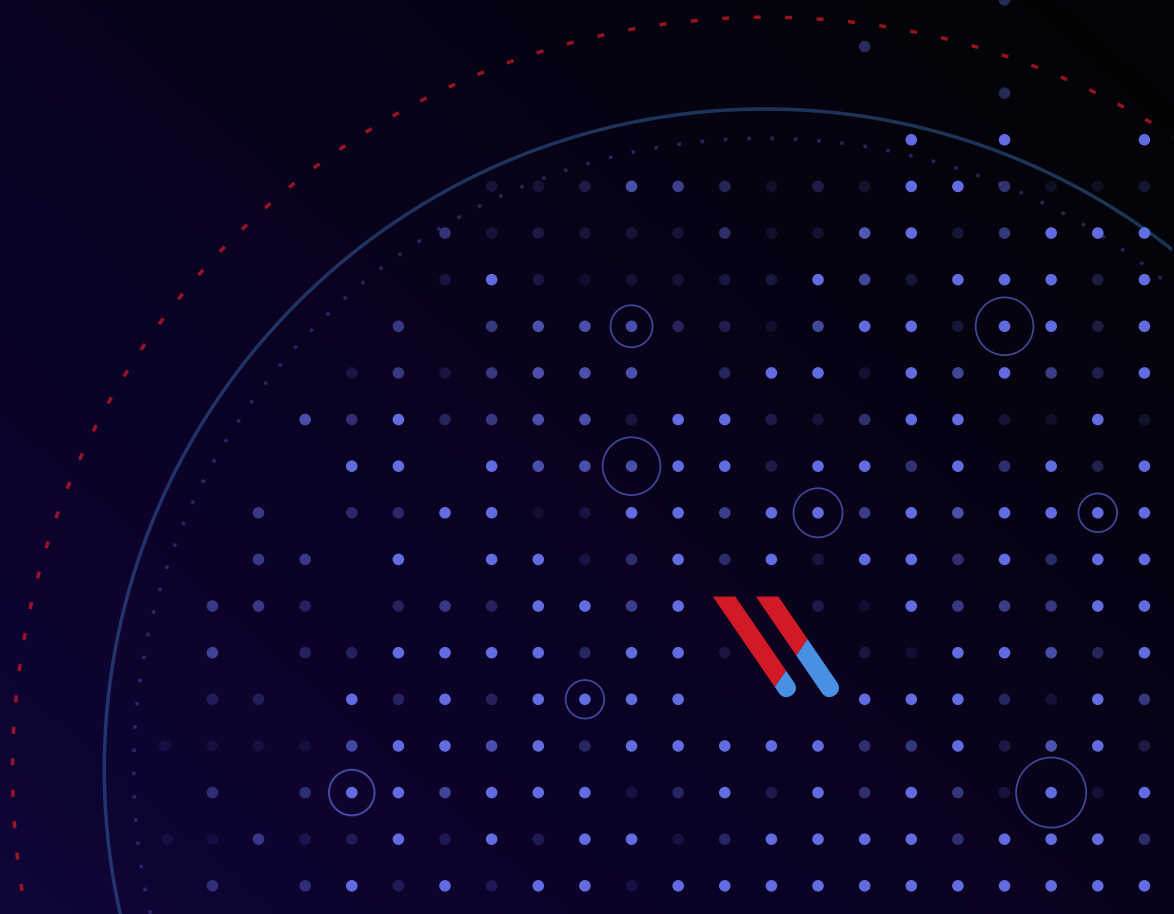
VARONIS

Varonis verfolgt ein anderes Ziel

Der einzigartige Cyber-Security-Ansatz von Varonis



Einleitung

Da Unternehmen fast ausschließlich datengesteuert arbeiten, speichern sie immer mehr Daten in lokalen und Cloud-Speichern, auf die Mitarbeiter dann von überall mit Telefonen, Tablets und Laptops zugreifen. Die Sicherheitsperimeter sind immer unklarer definiert, und die Endpoints austauschbar – sehr wenige Daten „leben" heutzutage nur auf einem Telefon oder Laptop.

Die digitale Transformation hat das traditionelle Sicherheitsmodell, das sich auf Perimeter und Endpoints konzentrierte, auf den Kopf gestellt. Anstatt sich auf die Richtung von außen nach innen zu konzentrieren, denken Unternehmen – im Rahmen der Data-First-Sicherheit – inzwischen immer mehr von innen nach außen.

Datenschutz ist intuitiv einfach, aber ungeheuer komplex.

Warum ist Datenschutz intuitiv einfach?

Ich würde argumentieren, dass Ihre Daten sicher sind, wenn Sie diese drei Fragen kontinuierlich mit „Ja" beantworten können:

1. Wissen Sie**, wo Ihre wichtigen Daten gespeichert sind?**
2. Wissen Sie**, dass nur nur die richtigen Leute Zugang dazu haben?**
3. Wissen Sie, **dass sie die Daten korrekt verwenden?**

Ganz einfach, oder?

Das sind die drei grundlegenden Dimensionen des Datenschutzes – Wichtigkeit, Zugänglichkeit und Nutzung. Wenn Sie in den Bereichen IT oder IT-Sicherheit arbeiten, ist Ihnen klar, dass das Verständnis dieser Dimensionen nicht einfach ist.

Wahrscheinlich wissen Sie auch, dass sie andere Fragen nach sich ziehen, die für CISOs, Compliance-Personal, Vorstände und Aktionäre wichtige Auswirkungen haben, falls Sie sie nicht mit ja oder überhaupt nicht beantworten können:

- Wo sind unsere sensiblen und regulierten Daten?
- Wo sind sie übermäßig zugänglich und am meisten gefährdet?
- Wie groß ist der mögliche Schaden durch ein kompromittiertes Konto oder einen kompromittierten Mitarbeiter?
- Wie könnten wir erfahren, ob Daten gestohlen, verschlüsselt oder gelöscht wurden?
- Können wir sie löschen?

Die Antworten werden nicht einfacher, da die Datenmengen sowohl lokal als auch in der Cloud, in Anwendungen und Datenspeichern, die jeweils ihre eigenen Sicherheitsmodelle haben, ständig wachsen. Es ist schon schwer genug, den Datenschutz in einer einzigen Unternehmensplattform korrekt aufrechtzuerhalten, geschweige denn in vielen gleichzeitig.

Wo sollten unsere Daten sein?

Die Anzahl der Orte, an denen wir Daten speichern können, hat in den letzten Jahren explosionsartig zugenommen und in der Regel können Benutzer auf ihre Daten über mehrere Geräte und Endpoints hinweg zugreifen. Endpoints dienen jetzt in erster Linie als Gateways zu dem Ort, an dem die Daten wirklich „leben“. In der Regel handelt es sich dabei um eine Cloud-Anwendung.

Die meisten verlassen sich aktuell auf eine Kombination aus Cloud-Anwendungen und -Infrastruktur, die ihre lokale Infrastruktur ergänzt. Immer häufiger nutzen Unternehmen für die Zusammenarbeit Microsoft 365, Box, Google Drive oder Slack, GitHub oder Jira für Quellcodes, AWS, Azure oder Google Cloud zur Auslagerung von Rechenleistung oder Speicher sowie eine CRM-Lösung wie Salesforce.com.

Wo sind die wichtigen Daten?

Selbst im Bereich solcher „genehmigter“ Anwendungen ist die Oberfläche groß, schwer zu visualisieren und kompliziert in der Risikobewertung. Einige Unternehmen konzentrieren ihre Bemühungen, indem sie ihre Mitarbeiter auffordern, Dateien zu taggen, oder indem sie Automatisierungen nutzen, um regulierte oder sensible Daten zu identifizieren oder zu klassifizieren. Die Hoffnung hierbei ist, dass sie so ihre Datenschutzbemühungen priorisieren können.

Es ist sicherlich sinnvoll, ein riesiges Problem in kleinere Teile zu zerlegen, aber das Problem ist so groß geworden, dass selbst die kleineren Teile überwältigend sein können.

Die meisten Unternehmen sind von der Anzahl an sensiblen Dateien und Datensätzen, die sie finden, überrascht. Tausende von Dateien hier – Tausende oder Zehntausende da – und schon morgen oder übermorgen ändert sich die Liste wieder.

Wenn man an diesem Punkt keinen klaren Aktionsplan hat, kann man schnell beim nächsten Schritt stecken bleiben. Manche denken über einen Brute-Force-Ansatz nach, beispielsweise alles, was man findet, woanders hin zu verschieben, z. B. in einen lokalen Speicher, oder alles zu löschen, was möglich ist, oder alles zu verschlüsseln und damit nur den Mitarbeitern oder einer kleinen Gruppe, die gerade ein großes Problem geerbt hat, zugänglich zu machen.

Dadurch wird das Kernproblem jedoch nicht wirklich gelöst – und zwar sicherzustellen, dass nur die richtigen Personen auf Daten zugreifen können –, auch bekannt als das Prinzip der notwendigsten Berechtigung oder als „Zero Trust“.

Um sicherzustellen, dass der korrekte Zugriff für alle Daten, sensibel oder nicht, gewährleistet ist, müssen Sie zunächst sehen können, wer Zugriff darauf hat – und das ist fast immer schwieriger, als man denken könnte, insbesondere in der Cloud.

Wer hat Zugriff auf unsere wichtigen Daten? Wer *sollte* Zugriff haben?

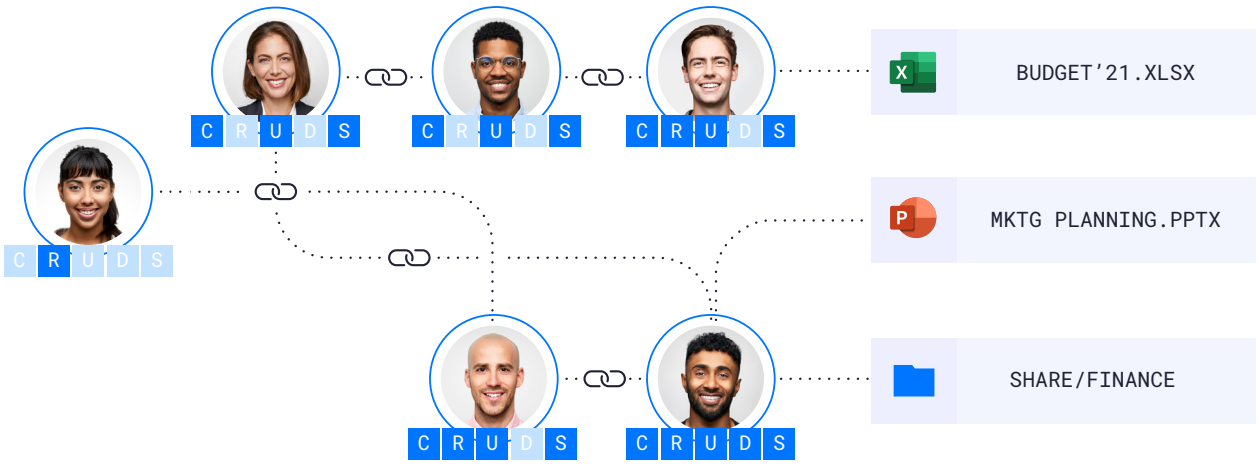
Es überrascht nicht, dass man, wenn man nicht weiß, welche Daten sensibel sind oder gesetzlichen Vorschriften unterliegen, Entscheidungen über den Zugriff treffen muss, ohne dabei sehr wichtige Kontextinformationen zu haben. Überraschend ist jedoch oft, wie schwierig es ist, in Erfahrung zu bringen, wer überhaupt Zugriff hat.

Der Zugriff auf Daten wird über Berechtigungen oder Access Control Lists geregelt. Die Logik ist über Anwendungen und Datenspeicher hinweg relativ einheitlich:

- Es gibt ein **Objekt** wie eine Datei, einen Ordner oder einen Datensatz.
- Es gibt **digitale Identitäten** die Benutzern, Konten und Gruppen von Benutzern und Konten entsprechen, die mit diesen Objekten arbeiten können.
- Es gibt eine **Beschreibung dessen, was sie tun können,** beispielsweise Erstellen, Teilen, Löschen usw.

Auch wenn die Logik in etwa die gleiche ist – egal ob bei Slack, Box, SharePoint Online, lokal oder bei UNIX-Dateisystemen – sind die Implementierungen alle unterschiedlich:

- Die Objekte sind ähnlich, jedoch gibt es je nach Anwendung unterschiedliche Objekttypen (z. B. Dateien, Standorte, Datensätze, Buckets).
- Benutzer/Konten und Gruppen werden an mehreren Orten gespeichert – in der Cloud hat jeder Datenspeicher normalerweise seine eigene Datenbank mit Benutzern und Gruppen. Manchmal sind sie mit anderen Konten verbunden (z. B. einem Okta-Konto), manchmal gibt es sowohl persönliche als auch Firmenkonten, die verfolgt werden müssen. Jede dieser Anwendungen kann den Benutzer- und Gruppenobjekten Attribute wie Titel, Rolle und Standort zuweisen.



Was sie tun können, wird in jeder Anwendung anders beschrieben, obwohl die möglichen Aktionen meist auf das Erstellen, Lesen, Aktualisieren, Löschen und Freigeben hinauslaufen.

Zusätzlich zu diesen Unterschieden kann die Berechnung von effektiven Berechtigungen für ein bestimmtes Objekt oder einen bestimmten Benutzer sehr komplex sein und sich je nach Speicher stark unterscheiden. Um die effektiven Berechtigungen für ein bestimmtes Objekt zu bestimmen, müssen mehrere Attribute berücksichtigt werden, darunter:

- **Objektspezifische Berechtigungen.** Wie oben erwähnt, hat jedes Objekt eine Access Control List, die Benutzer-, Gruppen- oder Rollenentitäten auflistet. Die Bandbreite der Möglichkeiten ist groß – bei grundlegenden UNIX-Berechtigungen gibt es z. B. 3 mögliche Berechtigungen (Lesen, Schreiben und Ausführen) für 3 Benutzer/Gruppen (Root, Eigentümer, Gruppe); in SharePoint online gibt es 33 mögliche Berechtigungen, die in 7 Standardstufen gruppiert sind (man kann zusätzliche erstellen), und diese Berechtigungsstufen können **vielen** Benutzern und Gruppen auf den Objekten zugewiesen werden.
- **Gruppenbeziehungen.** Gruppen können Benutzer oder andere „verschachtelte" Gruppen enthalten. Um die effektiven Berechtigungen für ein Objekt oder einen Benutzer zu bestimmen, müssen diese Beziehungen berechnet werden. In einigen Fällen können Gruppen in einem Verzeichnisdienst auf Benutzer und Gruppen in anderen Verzeichnisdiensten verweisen, wodurch diese Berechnung komplexer wird. SharePoint Online hat zum Beispiel lokale Gruppen, die Benutzer und Gruppen in Azure AD enthalten können.
- **Hierarchische Vererbung.** In vielen Datenspeichern fließen Berechtigungen durch die Hierarchien nach unten, sodass alle Objekte in einem Ordner Zugriffssteuerungseinträge von übergeordneten Elementen „erben". In manchen Speichern können Sie die Vererbung auf untergeordnete Objekte stoppen, aber nicht bei allen ist dies möglich. Box unterstützt beispielsweise nur das Hinzufügen von Zugriffssteuerungseinträgen für untergeordnete Objekte, sodass ein untergeordnetes Objekt nie weniger Berechtigungen aufweisen kann als seine übergeordneten Objekte.
- **Rollen und Rollenhierarchien.** Der Zugriff auf Objekte kann basierend auf einer Rolle gewährt werden. Rollen können andere Rollen enthalten und werden in verschiedenen Anwendungen unterschiedlich zugewiesen. In AWS werden Rollen beispielsweise in der Regel nach Bedarf übernommen, während Rollen in Salesforce eher statisch zugewiesen werden.
- **Systemweite Einstellungen.** Einige Einstellungen wirken sich auf den Zugriff auf alle Objekte aus. In Google Drive beispielsweise überschreibt die Linkfreigabe-Einstellung alle Berechtigungen und macht jedes neu erstellte Objekt für die gesamte Domäne zugänglich. In Salesforce legen die „Organisationsweiten Standardeinstellungen" (OWDs) den Zugriff auf Basisebene für alle Objekte fest.

Um den Zugriff zu visualisieren, müssen alle diese Attribute und funktionalen Beziehungen über Datenspeicher und Anwendungen hinweg vorab berechnet und normalisiert werden. Ohne eine solche Automatisierung ist es extrem zeitaufwändig zu ermitteln, wer Zugriff auf ein Objekt hat oder welcher Benutzer oder welches Konto Zugriff hat (der effektive mögliche Schaden bei einem Angriff). Außerdem werden dadurch die täglichen Aufgaben beeinträchtigt, von der Reaktion auf einen Vorfall über die Fehlerbehebung bis hin zu Audit-Berichten.

Ist es einfacher, Zugriffsaktivitäten zu verstehen als Berechtigungen?

Nein, das ist es nicht.

Bei der Datensicherheit gibt es mehrere Arten von Ereignissen, die sich direkt auf den Datenschutz beziehen.

- **Datenzugriffsereignisse.** Die sicherheitsrelevantesten Aktivitäten umfassen direkte Interaktionen mit Daten – wenn Benutzer Daten erstellen, lesen, ändern/aktualisieren, löschen oder freigeben. Leider hat jede Anwendung und jeder Datenspeicher seine/ihre eigene Art, die direkte Interaktion von Benutzern mit Daten aufzuzeichnen (oder nicht aufzuzeichnen). In Salesforce-Protokollen wird in der Datenzugriffsaktivität zum Beispiel aufgezeichnet, auf welches Objekt zugegriffen wurde.
- **Änderungen der Zugriffskontrolle und Konfigurationsänderungen**, die sich auf die Zugänglichkeit von Daten auswirken, sind ebenfalls von großer Bedeutung. Änderungen der Zugriffskontrolle werden unterschiedlich gemeldet und sind ohne Kenntnis der Benutzer und Gruppen, auf die sie sich beziehen, unvollständig. Viele Systeme, die Berechtigungen protokollieren, protokollieren beispielsweise nur, dass eine Access Control List (ACL) geändert wurde – nicht aber, welche Einträge geändert wurden. Außerdem werden Änderungen an den Objekten, auf die in der ACL verwiesen wird, möglicherweise nicht vom Dateisystem oder der Anwendung aufgezeichnet – diese müssen eventuell im Verzeichnisdienst (z. B. Azure Active Directory) aufgezeichnet werden. Konfigurationsänderungen sind ähnlich komplex, sogar in Bezug auf die Datenzugänglichkeit. GPO-Änderungen in Active Directory können sich auf alle möglichen wichtigen Aspekte auswirken, wie Kennwortrichtlinien und Endpunktfunktionen. GitHub zum Beispiel zeichnet Änderungen an der Zugänglichkeit von Code-Repositories auf, gibt aber nicht an, welche Änderungen genau vorgenommen wurden.
- **Authentifizierungsereignisse** können einen aussagekräftigen Kontext darüber liefern, welche Benutzer sich mit der Anwendung oder dem Datenspeicher verbunden haben, von wo aus und mit welcher Art von Authentifizierung (z. B. Single- oder Multi-Factor-Authentifizierung). Authentifizierungsereignisse unterscheiden sich je nach Verzeichnisdiensten und Anwendungen.
- **Perimeterereignisse.** In einer lokalen Infrastruktur bieten Perimetersignale von DNS, VPN-Gateways und Proxies Einblicke in ungewöhnliche Verbindungen in und aus der Umgebung. Ereignisse von Perimetergeräten sind umfangreich und nicht einheitlich – es kann verlockend sein, Telemetrie von vielen Orten zu nutzen, aber man muss aufpassen, dass dabei nicht zu viele unbrauchbare Informationen anfallen. Am praktischsten ist Telemetrie, die aus der Datenperspektive relevant ist, beispielsweise DNS, um Infiltration zu sehen, und Web-Proxy, um Exfiltration zu sehen. Weitere Informationen finden Sie unter **5 Arten, auf die Ihr SIEM versagt**.

Da Datenspeicher und Anwendungen diese Ereignisse so unterschiedlich beschreiben, ist es sehr schwierig, Fragen übergreifend zu beantworten. Nur um zu verstehen, auf welche Daten ein Mitarbeiter an einem bestimmten Tag zugegriffen hat oder welche Zugriffssteuerungsänderungen ein Administrator vorgenommen hat, muss man ganze Forschungsprojekte statt einfacher Abfragen durchführen.

Wie sieht es mit Alarmen aus?

Ohne einen einheitlichen, normalisierten Ereignisstrom ist die regelbasierte Alarmierung schwer zu bewerkstelligen, und die verhaltensbasierte Alarmierung ist entweder auf eine einzige Anwendung beschränkt oder komplett unmöglich. Bei der Verhaltensmodellierung zur Erstellung von Profilen müssen die Ereignisse auch ergänzt werden, damit die KI eine sinnvolle Gruppe von Facetten zur Bewertung hat. Wenn Sie beispielsweise einen einfachen schwellenwertbasierte Alarm erstellen möchten, der ausgelöst wird, wenn jemand innerhalb von fünf Minuten mehr als 1.000 Dateien oder Objekte löscht, aktualisiert oder darauf zugreift, müssten Sie ohne einen zuverlässigen, einheitlichen Ereignisstrom wahrscheinlich für jede Anwendung einen Alarm erstellen. Wenn dieser Alarm ausgelöst werden soll, falls die Gesamtzahl der Ereignisse 1.000 Dateivorgänge in einem Zeitraum von 5 Minuten in allen Speichern überschritten hat, muss man dafür bereits relativ fortgeschrittene Abfragen schreiben.

Wenn man nun etwas weiter gehen möchte, z. B. einen Alarm erzeugen, wenn innerhalb von 5 Minuten über alle Datenspeicher hinweg auf 1.000 sensible Dateien zugegriffen wird, muss man die Ereignisse mit Informationen zur Dateisensibilität ergänzen, bevor sie von der Alarm-Logik verarbeitet werden. Man kann sehen, wie wichtig saubere, ergänzte Ereignisse bei schwellenwertbasierten Alarmen sind – für KI-gesteuerte Alarme sind sie sogar noch wichtiger.

Saubere, ergänzte Ereignisströme sind der Schlüssel zum Aufbau von Verhaltensbaselines oder Peace-Time-Profilen („Friedenszeit"-Profilen), anhand derer die KI Abweichungen bewerten kann. Diese datenzentrierten Profile ergeben Alarme, mit einem sehr hohen Maß an Signal-Rausch-Verhältnis. Wenn beispielsweise eine Führungskraft, die normalerweise auf ein Dutzend Dateien pro Woche zugreift, von denen nur wenige wichtig sind, auf einmal auf Dutzende von wichtigen Dateien zugreift, auf die weder sie noch ihre Kollegen zugreifen – vielleicht auch noch von einem Gerät, das diesem Benutzer nie zugeordnet wurde, oder von einem Ort aus, den er normalerweise nicht besucht – erfordert das sofortige Aufmerksamkeit.

Die Verhaltensanalyse erfordert relevantes, ergänztes und zuverlässiges Verhalten, das analysiert werden kann. Aus diesem Grund versagen Sicherheitstechnologien zwangsläufig, die unzuverlässige, verrauschte Datenströme analysieren.

Ohne drei Dimensionen **kommt man nicht weit**

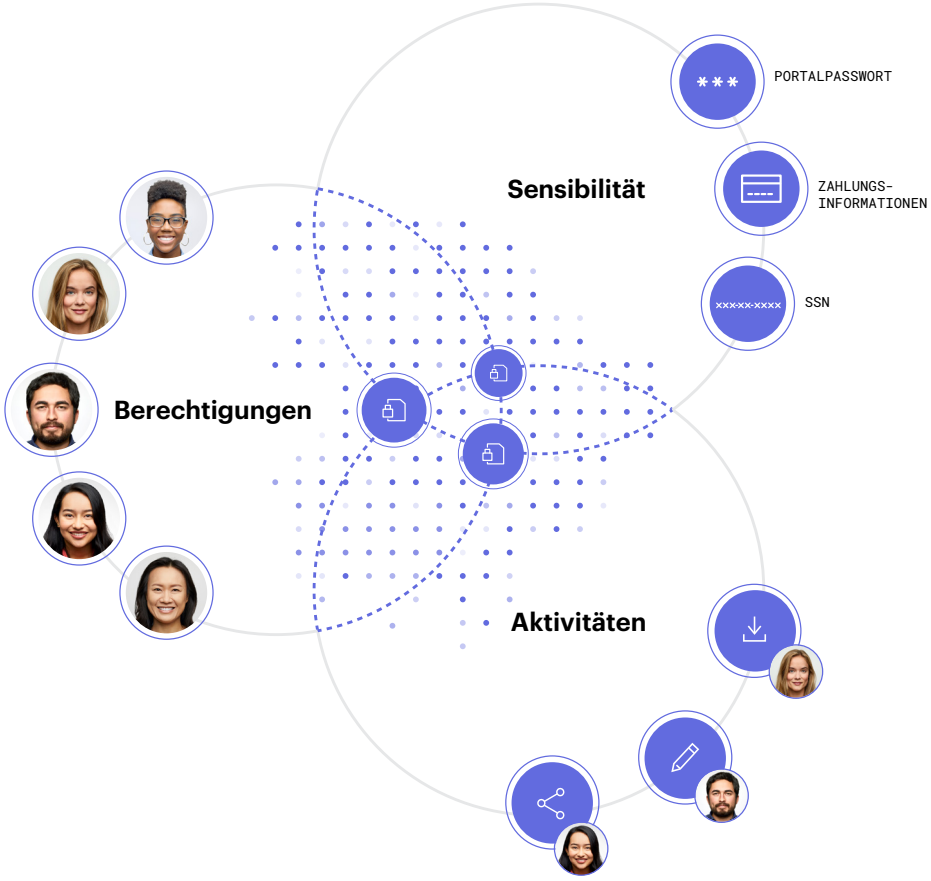
Wenn sie eine der drei bisher besprochenen Dimensionen – Sensibilität, Berechtigungen und Aktivitäten – nicht sehen können, denken viele, dass sie mit nur einer oder zwei Dimensionen auskommen. Wenn wir jedoch die verschiedenen Kombinationen untersuchen, erkennen wir schnell, wie viel leistungsfähiger es ist, alle Dimensionen zu kombinieren.

Wie ich bereits erläutert habe: Wenn man nur weiß, welche Daten sensibel sind, weiß man noch nicht, wo sie konzentriert sind oder wo sie offenliegen, solange man die Dimension der Berechtigungen nicht mit einbezieht. Ohne Aktivitäten weiß man nicht, wie man eine gefundene Offenlegung sicher beheben kann oder ob vertrauliche Daten gestohlen wurden, oder mit wem man darüber sprechen soll. Wenn man nur die Aktivitäten sieht, kann man zwar sehen, welche Daten nach einer Verletzung gestohlen wurden, oder sogar auf Verhaltensabweichungen hinweisen. Man weiß aber nicht, wie vertraulich die Daten waren, wer sonst noch darauf Zugriff hatte, oder ob sie inkorrekterweise für alle Personen im Unternehmen (oder im Internet) offenlagen.

Beim Datenschutz sind alle diese Dimensionen erforderlich, um die kritischen Fragen zu beantworten, mit denen dieses Dokument begonnen hat:

1. Wissen Sie**, wo Ihre wichtigen Daten gespeichert sind?**
2. **Haben nur die richtigen Personen Zugriff?**
3. Wissen Sie, dass **sie die Daten richtig verwenden?**

Wenn wir diese Fragen durchgehend mit „Ja“ beantworten können, können wir auch die wichtigste Frage von allen mit „Ja“ beantworten: **„Sind unsere Daten sicher?“**



VARONIS

VARONIS

Sind Sie bereit, zu sehen, was Varonis anders macht?

Reduzieren Sie Ihr Risiko, ohne eines einzugehen. Setzen Sie sich mit unserem Team in Verbindung, um zu erfahren, was in Ihrem **kostenlosen** Data Risk Assessment enthalten ist.

Kontakt

ÜBER VARONIS

Varonis ist ein Pionier im Bereich Datensicherheit und Analytik, und kämpft an anderer Front als die herkömmlichen Cybersicherheitsanbieter. Varonis ist spezialisiert auf den Schutz von Unternehmensdaten in lokalen Systemen und in der Cloud: sensible Dateien und E-Mails, vertrauliche Kunden-, Patienten- und Mitarbeiterdaten, Finanzdaten, strategische Pläne und Produktpläne sowie sonstiges geistiges Eigentum.

Die Datensicherheitsplattform von Varonis erkennt Insider-Risiken und Cyberangriffe durch Analysieren von Daten, Kontoaktivitäten und des Benutzerverhaltens, beugt durch Sperren und Einschränken sensibler und veralteter Daten Katastrophen vor und sorgt durch Automatisierung für einen sicheren Zustand. Varonis eignet sich für zahlreiche Zielsetzungen mit Schwerpunkt auf Datensicherheit, einschließlich Governance, Compliance, Klassifizierung und Bedrohungsanalyse. Varonis hat seine Geschäftstätigkeit im Jahr 2005 aufgenommen und hat Tausende Kunden weltweit – darunter Branchenführer aus den Bereichen Technologie, Konsumgüter, Handel, Finanzdienstleistungen, Gesundheitswesen, Manufacturing, Energie, Medien und Bildung.