

Blank ist Vertrauen

In der heutigen informationsüberladenen Welt wird deutlich, wie einst benötigte Daten zu einer Bedrohung für Ihr Unternehmen werden können.



“Im März 2022 gab ein neuseeländischer Reiseveranstalter bekannt, dass es zu einer schwerwiegenden Datenschutzverletzung gekommen war. Durch diese Verletzung wurden die über 15 Jahre gesammelten personenbezogenen Daten von Hunderttausenden von Kunden offengelegt”

Erfahren Sie, wie Sie das Risiko minimieren können, das durch das Festhalten an alten Daten entsteht.

Wir produzieren heute täglich Hunderte von Millionen Terabyte an Daten. Viele dieser Informationen sind für die Personalisierung von Diensten, die Vorhersage von Risiken, die Analyse von Geschäftszielen und die Entwicklung von Strategien unerlässlich. Datengesteuerte Analysen sind zwar nichts Neues, aber unsere Fähigkeit, so viele Informationen zu sammeln, schon. Es ist sehr nützlich, all diese Details zur Hand zu haben.

Bis sie es nicht mehr sind. Dann liegen diese Daten vergessen in Netzwerken oder Laufwerksspeicherumgebungen. Sie werden zu einer tickenden Zeitbombe, die nur darauf wartet, einen Verstoß gegen die Vorschriften oder eine Datenschutzverletzung zu verursachen.

Leer ist vertrauensbildend, denn wenn sensible Dateien oder Ordner verschwunden sind, sind sie auch weg. Die Informationen können nicht in die Hände böswilliger Akteure gelangen, weil sie nicht mehr vorhanden sind.

Bleibt er dagegen zurück und wird nicht ordnungsgemäß verwaltet, drohen Geldstrafen in Millionenhöhe und ein unermesslicher Vertrauensverlust bei den Kunden.

Die Speicherung von Informationen ist für viele Unternehmen zu einem zweiseitigen Schwert geworden, da sie den Wert der Daten mit der potenziellen Haftung abwägen müssen. Während viele Daten als eine Art digitales Gold bezeichnen, zeigen zwei aktuelle Fälle, wie unsachgemäße Informationsspeicherung und mangelhafte Praktiken zur Datenlöschung in Unternehmen zu einem teuren Gerichtsverfahren und einer hohen Geldstrafe führten.

Sicherheitslücke offenbart PII des Kundenstamms einer neuseeländischen Vereinigung

Im März 2022 gab ein neuseeländischer Reiseveranstalter bekannt, dass er von einer schwerwiegenden Datenschutzverletzung betroffen war. Durch diese Verletzung wurden die über 15 Jahre hinweg gesammelten personenbezogenen Daten von Hunderttausenden von Kunden offengelegt.

Zu den gestohlenen Informationen gehörten Namen, Adressen, Kontaktinformationen und abgelaufene Kreditkartennummern aus einer Abteilung der Vereinigung, die 2018 ihren Betrieb einstellte.

Anstatt die nicht mehr benötigten Daten zu löschen, behielt der Verband die Kundeninformationen auf den angeschlossenen Servern. Hätte das Unternehmen Methoden zur Datenbereinigung angewandt und nicht mehr benötigte Informationen dauerhaft entfernt, hätte

es diese Situation vermeiden können.

Die Führungskräfte des Unternehmens bestätigten dies, und die amtierende neuseeländische Datenschutzbeauftragte Liz Macpherson stimmte dem zu.

“Die Unternehmen brauchen eine Überprüfungsstrategie, um festzustellen, ob die gespeicherten Daten notwendig waren”, sagte sie und fügte hinzu, dass die Unternehmen die Datenerfassung auf ein Minimum reduzieren müssen.

Wenn zu viele Daten gesammelt und nicht ordnungsgemäß gelöscht werden, haben böswillige Akteure die Möglichkeit, eine Identität herzustellen.

Verstoß gegen die Datenschutzgrundverordnung führt zu einer hohen Geldstrafe für dänisches Finanzinstitut

Im zweiten Fall wurde eine dänische Bank zu einer Geldstrafe in Höhe von 1,5 Millionen Dollar (1,3 Millionen Euro) verurteilt, weil sie die EU-Richtlinien zur Datenschutz-Grundverordnung (DSGVO) zum Recht auf Löschung von Daten nicht eingehalten hatte.

Die Datenschutz-Grundverordnung verlangt, dass personenbezogene Daten von Dienstleistern gelöscht werden, wenn Dienstleistungen enden oder rechtliche Vereinbarungen auslaufen. Die wichtigsten Ergebnisse der dänischen Aufsichtsbehörde zeigten jedoch, dass die Bank “nicht in der Lage war zu dokumentieren, ob Regeln für die Löschung und Speicherung personenbezogener Daten festgelegt wurden oder ob eine manuelle Löschung personenbezogener Daten durchgeführt wurde”.

Es gab zwar keinen Verstoß, aber die Bank bewahrte die Kundendaten länger auf, als es die Vorschriften zuließen.

The bank faced a challenge that many organizations encounter: A distributed network of technology systems that made it difficult to build the right functionality. The organization found itself incapable of keeping up with data destruction demands in its more than 400 individual banks. Collectively, these banks process the personal data of millions of people.

Erfahren Sie mehr über die Datenlöschlösungen von Blanco:
[VIDEO] Datenlöschlösungen von Blanco



Warum Unternehmen Daten speichern

Unternehmen bewahren sensible Daten aus vielen Gründen zu lange auf:

- Möglicherweise möchten sie die Daten für die künftige Verwendung aufbewahren, auch wenn sie nicht wissen, wie das aussehen würde.
- Einigen Unternehmen fehlt es an Software zur Datenlöschung oder sie sind mit den entsprechenden Verfahren zur ordnungsgemäßen Löschung von Daten nicht vertraut.
- Andere glauben, dass die Daten sicher bleiben werden.

Die Speicherung unnötiger Daten hat jedoch Folgen.

Die Aufbewahrung älterer Daten birgt Risiken für Verstöße und Strafen, die sich nicht lohnen

Der IBM Annual Cost of a Data Breach Report

zeigt, dass die durchschnittlichen Kosten für Datenschutzverletzungen im Jahr 2022 bei 4,35 Millionen US-Dollar liegen, 2,6 Prozent mehr als 2021 und 12,7 Prozent mehr als 2020. Neben den Kosten für die Behebung und Schadensbegrenzung können Unternehmen im Falle einer Datenschutzverletzung je nach Anzahl der kompromittierten Daten haftbar gemacht werden.

Unnötige Daten, die nicht ordnungsgemäß aus dem Speicher oder den aktiven Netzwerken entfernt werden, bleiben angreifbar. Sogar auf Daten, die auf abgeschalteten Servern des Rechenzentrums und stillgelegten mobilen Geräten gespeichert sind, kann unter bestimmten Umständen zugegriffen werden.

Zusätzlich zu Verstößen gegen die DSGVO können bestimmte Arten von Verstößen zu **Geldbußen führen**. Diese Geldbußen können bis zu 20 Mio. EUR oder 4 % des weltweiten Jahresumsatzes des Unternehmens aus dem vorangegangenen Geschäftsjahr betragen, je nachdem, welcher Betrag höher ist.

Anstatt diese Risiken einzugehen, benötigen Unternehmen ein proaktives, überprüfbares und zertifiziertes Verfahren zur dauerhaften Vernichtung unnötiger Daten.

Auf diese Weise kann sichergestellt werden, dass diese Daten unzugänglich gemacht werden, was das Risiko reduziert, das Vertrauen der Kunden aufrechterhält, potenzielle Geldstrafen vermeidet und das Risiko von Datenschutzverletzungen begrenzt. Eine solche Datenlöschung stellt auch sicher, dass eine Organisation alle nationalen, regionalen und marktspezifischen Vorschriften einhält.

Bewährte Verfahren zur Datenlöschung in Unternehmen

Die zunehmende Zahl von Datenschutzgesetzen wird vielen Organisationen einen Rahmen für die Verwaltung herausragender Daten bieten.

Die Datenschutz-Grundverordnung (GDPR) ist vielleicht die bekannteste, aber mehr als 100 Länder haben [spezifische Gesetze](#), die Organisationen befolgen sollten.

Maßnahmen, die Sie ergreifen können, um das Risiko durch alte Daten zu minimieren:

- 1. Machen Sie sich mit den branchenspezifischen und staatlichen Vorschriften** zur Speicherung, zum Schutz und zur Löschung von Daten vertraut. Die Befolgung von Vorschriften wie der GDPR kann als solider Leitfaden dienen. Sie können die Art und Weise, wie Unternehmen sensible Geschäfts- und Verbraucherdaten schützen, verbessern. Dies gilt insbesondere für Organisationen, die nicht über branchenspezifische Vorschriften wie [PCI DSS](#), [HIPAA](#), und [NCSC](#) und viele andere verfügen.
- 2. Überprüfen Sie Ihre Datenspeicherung.** Unabhängig von diesen Vorschriften sollten Sie Ihre Daten regelmäßig überprüfen, um festzustellen, welche Daten keinen Wert mehr haben. Doppelte Daten, veraltete Kundeninformationen, Informationen, die das vorgeschriebene Aufbewahrungsdatum () überschritten haben, oder Informationen, die sich auf ein nicht mehr existierendes Unternehmen beziehen, sollten die Hauptkandidaten für die Datenlöschung sein. [Eine bahnbrechende Studie](#) zeigt, dass 85 Prozent der Daten veraltet sein könnten.
- 3. Trennen Sie sich von dem, was Sie nicht brauchen.** Sobald Sie festgestellt haben, welche Daten überflüssig, veraltet oder trivial sind, sollten Sie skalierbare, zertifizierte Datenlöschungsmethoden einsetzen, um die dauerhafte Vernichtung dieser Daten zu gewährleisten, selbst in komplexen Netzwerken. Wenn Sie dies nicht tun, kann dies zu zusätzlicher Haftung, Risiken und Stress führen, ohne dass Sie dafür einen entsprechenden Gegenwert erhalten.

Es ist wichtig, nicht nur die Daten in Ihren Rechenzentren oder Cloud-Umgebungen zu berücksichtigen, sondern auch Daten, die auf Endbenutzergeräten, Remote- und Bürogeräten gespeichert sind, insbesondere wenn Mitarbeiter oder Auftragnehmer regelmäßig mit sensiblen persönlichen Daten Ihrer Kunden und Mitarbeiter oder sogar mit geschützten Informationen Ihres Unternehmens umgehen.

Wenn Sie sich um Ihre Daten kümmern, wenn sie nicht mehr benötigt werden, sind Sie einen Schritt weiter, um das Risiko von Datenschutzverletzungen und potenziellen Bußgeldern für die Nichteinhaltung von Vorschriften in der heutigen Zeit zu minimieren.

Die Blanco-Perspektive

Blank ist zuversichtlich, denn Daten sind erst dann wirklich sicher, wenn sie für immer verschwunden sind. Selbst die besten, am besten organisierten Unternehmen können Opfer von Compliance-Verstößen oder Datenschutzverletzungen werden, wenn sie die

Daten vergessen, die sie nicht mehr benötigen. Eine regelmäßige, nachvollziehbare Datenbereinigung mindert diese Gefahren und ermöglicht es Ihnen, die Chancen zu nutzen, die unsere informationslastige Umgebung bietet.

Beginnen Sie mit der Priorisierung der Datenbereinigung

Gewinnen Sie Vertrauen in Ihre Data-Governance-Praktiken. Erfahren Sie mehr über die Gefahren, die eine unnötige Datenspeicherung mit sich bringt, indem Sie sich in unserem Content Hub umsehen.

Besuchen Sie unseren Content Hub