



DATENSCHUTZ NEU ÜBERDACHT

RISIKOBETRACHTUNG UND INVESTITIONSLEITFADEN
FÜR IT-VERANTWORTLICHE

FREEFORM DYNAMICS, JANUAR 2018

DATENSCHUTZ – ZWÄNGE UND CHANCEN

Mit der Digitalisierung der Wirtschaft und der ganzen Welt wächst der Druck auf IT-Verantwortliche, durch effektive Verwaltung und effektiven Schutz der elektronischen Daten ihrer Organisation betriebliche und geschäftliche Risiken zu minimieren. In der wachsenden Abhängigkeit von Daten liegt zugleich die Chance, das Datenmanagement und den Datenschutz zu verbessern. Dies gilt umso mehr, weil Ransomware und die Datenschutz-Grundverordnung (DSGVO) von Budgetverantwortlichen ein aktives Datenmanagement erfordern. Ein Blick auf die wichtigsten Anforderungen zeigt dies.

Generelle Anforderungen Geschäftliche Sicht

Sicherheit und Zugriff

Stellen Sie sicher, dass nur berechtigte Personen Zugriff auf vertrauliche Daten haben.

Datenverlust vorbeugen

Vermeiden Sie Datenverlust durch menschliches Versagen, technologische Fehler oder Vorsatz.

Geschäftskontinuität

Sorgen Sie dafür, dass kritische IT-Systeme bei datenbezogenen Vorfällen und Ausfällen weiterlaufen.

Disaster Recovery

Minimieren Sie die Zeit für die Wiederherstellung Ihrer Systeme nach schwerwiegenden Fehlern.

Zunehmende Relevanz Schutz vor Ransomware

Eine Infektion mit einem datenverschlüsselnden Virus kann schwere Folgen haben. Neuere Exemplare sind netzwerkfähig und können Server und Cloud-Speicher beschädigen oder Backup-Medien verschlüsseln. Ransomware-Abwehr muss daher auf mehreren Ebenen erfolgen, inkl. Benutzertraining, Antivirensoftware, Netzwerk-Verhaltensanalyse etc. Wird man infiziert, ist die Zahlung eines Lösegelds nicht die Lösung. Der einzig zuverlässige Weg ist ein offline oder anderweitig geschütztes Backup.

Generelle Anforderungen Rechtliche und Compliance Sicht

Integrität von Aufzeichnungen

Sorgen Sie für genaue und vollständige Aufzeichnungen, um die gesetzlichen Berichtspflichten zu erfüllen.

Data Governance

Setzen Sie Richtlinien für die Erfassung, Speicherung, Verwendung, Aufbewahrung und Entsorgung von Daten um.

Informationsrecherche

Stellen Sie sicher, dass sich wichtige Daten je Kunde, Vorfall, Fall usw. schnell finden und wiederherstellen lassen.

Prüfung und Nachverfolgung

Sorgen Sie dafür, dass für Schlüsseldaten z. B. Erstellung, Zugriff, Änderung und Löschung, nachvollziehbar sind.

Neue Anforderung Einhaltung der DSGVO

Die neue EU-Verordnung zur Verarbeitung personenbezogener Daten tritt im Mai 2018 in Kraft. Für die meisten Organisationen bedeutet sie erhebliche Änderungen bei der Verwaltung von Daten. Das gilt insbesondere für die Transparenz und Rechenschaftspflicht – und kann bis zu Änderungen bei den Datensicherungssystemen reichen. In vielen Fällen könnte und sollte dies ein Anlass sein, die Datenschutzstrategie grundlegend zu überdenken.

Vom Risikomanagement zum zusätzlichen Geschäftswert

Beim Schutz von Daten zählt vor allem, dass Sie mit Ihren Daten arbeiten können. Ganz gleich, wie viele Backups Sie machen und in wie vielen Formaten – es bringt Ihnen nichts, wenn Sie beschädigte, verlorene oder archivierte Daten nicht innerhalb eines angemessenen Zeitraums wieder herstellen können.

Darüber hinaus gibt es sowohl geschäftliche Risiken als auch Chancen. Bilden die Datensicherungssysteme das Hub, über das man alle Daten eines Unternehmen findet, können sie bei der Risikominimierung und Erschließung neuer Chancen eine Schlüsselrolle übernehmen. Dies wiederum bietet auch die Möglichkeit, die IT und den Datenschutz in den Mittelpunkt des Geschäfts zu rücken.

IT-Abteilungen können mit Datensicherungssystemen nicht nur Risiken minimieren und Anforderungen erfüllen, sondern sie auch für weitere Aufgaben nutzen – beispielsweise für die Konsolidierung von Daten für Geschäftsanalysen, zum Erzeugen synthetischer Backups aus einem Archiv oder um Dark Data (also Daten, die für das Unternehmen vielleicht unsichtbar sind, weil sie sich z. B. auf dem Gerät eines Benutzers befinden, aber erheblichen geschäftlichen Nutzen haben) zu identifizieren und zu schützen. Dabei wird ein Datensicherungssystem mit jedem „Mehrwert“ wirtschaftlicher und effizienter.

MODERNE DATENSCHUTZLÖSUNGEN

Datenschutz ist mehr als nur Backup oder Backup und Archivierung – er deckt vielmehr ein breites Spektrum an Informationsmanagement- und Sicherheitsanforderungen ab. Moderne Lösungen bieten dafür viele Funktionen, die bei traditionellen Backup-Lösungen noch separat implementiert werden mussten.

Ideal ist ein integriertes System, das die vielfältigen Datenschutzrisiken und -anforderungen abdecken kann. Auswahl und Implementierung erfordern aber Zeit und Geld. Ransomware und die DSGVO erhöhen jedoch den Druck, rasch zu handeln – viele Organisationen planen daher entsprechende Budgets ein. Die Herausforderung besteht nun darin, Gelder nicht für weitere Insellösungen zu verschwenden, die zwar kurzfristig eine Lösung bieten, langfristig aber die Komplexität und Betriebskosten erhöhen.

Glücklicherweise sind die Anforderungen und Erwartungen von Organisationen ziemlich identisch, obwohl die Einzelheiten bei der Umsetzung zum Teil stark voneinander abweichen können. Auch wenn es nicht auf jeden einzelnen Fall zutrifft – hier sind einige Anforderungen und zentrale Themen, die man berücksichtigen und bei potenziellen Lieferanten hinterfragen sollte.

Datenschutzanforderungen

Geschäftsbetrieb

Sicherheit und Zugriff, Verhinderung von Datenverlust, Geschäftskontinuität, Disaster Recovery, Ransomware-Schutz

Recht und Compliance

Datenintegrität, Data Governance, Informationsrecherche, Prüfung und Nachverfolgung, Einhaltung der DSGVO

Zentrale Fragen und Überlegungen

Datenrecherche

Alle Daten auffindbar? Wie umgesetzt? Wie anpassungsfähig? Wie geschützt?

Datenklassifizierung

Welche relevant? Wie sensibel? Änderungen im Zeitverlauf? Ist der Schutz ausreichend?

Wiederherstellung

Tests in Granularitäten (Datensatz, Datei, VM usw.) möglich? Als Self-Service möglich?

Audits und Reporting

Zugriff auf sensible Daten nachverfolgbar? Warnungen bei fehlgeschlagenen Backups? Chargeback?

Richtlinienverwaltung

Wie einfach können Schutzstufen definiert und geändert werden?

Datensicherheit/-integrität

Können einzelne Backups verschlüsselt werden? Wie werden die Schlüssel verwaltet?

Hybride Wiederherstellung

Wiederherstellung auf unterschiedlichen Plattformen möglich, z. B. von On-Premise in die Cloud?

Wiederverwendung von Metadaten

Schutz und Wiederverwendung von Metadaten möglich, z. B. um sie für Analysen zu nutzen?

Beschaffungsmöglichkeiten

Selbst installieren, Auftragsfertigung (BTO), Appliance oder Managed Service?

Das Wichtigste nicht vergessen: Sicherheit, Zugriff, Automatisierung und Auditierung

Ganzheitlich betrachten, prüfen und planen

Wie bereits skizziert, umfasst Datenschutz zahlreiche Anforderungen, Services und Prozesse – und diese können sowohl sehr unterschiedlich sein als auch voneinander abhängen und miteinander verknüpft sein. Zum Beispiel ist ein Backup kein Archiv, aber ein modernes Datensicherungssystem kann als Archiv, Backup, datenschutzkonformer Speicher und anderes mehr dienen. Natürlich können Sie all solche Dienste auch als separate Lösungen implementieren. Und wahrscheinlich mussten Sie dies auch bereits tun, weil Anforderungen nach und nach auftraten. Doch der Aufwand vervielfacht sich dadurch ebenso wie der Speicherbedarf, weil unterschiedliche Systeme mehrere Kopien der selben Daten für unterschiedliche Zwecke speichern.

Normalerweise ist eine ganzheitliche Betrachtung mit sehr viel Aufwand verbunden, denn nicht jede weitere Service- oder Sicherheitsanforderung rechtfertigt grundlegende Änderungen. Bei der DSGVO und dem Schutz vor Ransomware ist das allerdings etwas anders. Insbesondere die DSGVO erfordert ein Handeln. Insofern überrascht es auch nicht, dass viele Organisationen hier erhebliche Mittel bereitstellen oder bereitstellen sollten.

Eine echte Chance besteht darin, diese Mittel so einzusetzen, dass man die Komplexität reduziert und zugleich andere Probleme löst. Mit einem modernen Datensicherungssystem und seinem hochentwickelten Datenmanagement, das garantiert weitaus leistungsstärker sein wird als Ihre derzeitigen Systeme, ist dies möglich. Zudem können Sie nach neuen Geschäftsmöglichkeiten suchen – z. B. nach neuen Möglichkeiten, die Daten Ihrer Organisation zu nutzen (natürlich im Rahmen der gesetzlichen und behördlichen Vorschriften). Es ist daher sinnvoll, seinen Datenschutz umfassend auf den Prüfstand zu stellen und mit einem neuen System so viele Themen wie möglich abzudecken.

Mittel bereitstellen, Lösungen implementieren

Es ist naheliegend, dass die IT bei der Spezifizierung, Anschaffung und Implementierung von Datensicherungssystemen federführend ist. Nicht vergessen darf man allerdings, dass viele der Risiken und Anforderungen sehr geschäftsrelevant sind. Die IT muss daher sicherstellen, dass alle Anliegen im Unternehmen – z. B. bei der Definition von Risikoprofilen und Schutzgraden (RTO/RPO) – berücksichtigt werden. Ebenso wichtig ist, dass ein einheitliches Verständnis bezüglich Compliance, Governance und der generellen Risikobereitschaft der Organisation entwickelt wird.

Die IT muss auch eng in den Aufbau der entsprechenden Prozesse einbezogen werden: Denn, wenn Systeme und Prozesse nicht passen, könnte eine Investition in die Datensicherungstechnologie nutzlos werden.

Darüber hinaus muss das Unternehmen wissen, dass es für seine Daten rechtlich verantwortlich ist. Auch wenn die IT die Basis für den Datenschutz implementiert und pflegt – die DSGVO regelt klar und deutlich, dass beispielsweise Fehler im Datenschutz in der Verantwortung der Geschäftsleitung liegen und, dass der Datenschutzbeauftragte die Befugnis haben muss, seiner Verantwortung nachzukommen.

Letztlich geht es auch darum, wie viel Zeit und Aufwand man für die Beschaffung und Implementierung der erforderlichen Hardware und Software investieren muss. Viele IT-Abteilungen wandeln sich von Technikern zu Experten für die Lösung komplexer Geschäftsprobleme mit Technologien. In diesem Zusammenhang muss man die potenziellen Vorteile einer selbst aufgebauten und integrierten Lösung (z. B. größere Kontrolle über den Prozess und die Konfiguration) gegen die Geschwindigkeit und Einfachheit des Kaufs eines kompletten Systems (als Appliance oder BTO) abwägen.

ÜBER FREEFORM DYNAMICS

Freeform Dynamics ist ein Analyst der IT-Industrie. Durch unsere Forschung und Erkenntnisse wollen wir stark eingespannte IT- und Geschäftsverantwortliche dabei unterstützen, mit der schnellen technologischen Entwicklung Schritt zu halten und ihnen helfen, fundierte Investitionsentscheidungen zu treffen.

Besuchen Sie uns für nähere Informationen und für unsere frei verfügbaren Studien auf www.freeformdynamics.com.

ÜBER FUJITSU

Fujitsu ist führender japanischer Anbieter von Informations- und Telekommunikations-basierten (ITK) Geschäftslösungen mit einer breiten Palette an Technologieprodukten, -lösungen und -dienstleistungen. Mit rund 162.000 Mitarbeitern betreut Fujitsu Kunden in mehr als 100 Ländern. Wir nutzen unsere ITK-Expertise, um die Zukunft der Gesellschaft gemeinsam mit unseren Kunden zu gestalten.

Dazu gehört ein umfassendes Portfolio von Datensicherungslösungen, mit dem wir es Kunden ermöglichen, Daten auf einfache und effiziente Weise zu sichern, wiederherzustellen und zu archivieren.

Dieses Dokument wurde im englischen Original von Freeform Dynamics Ltd. verfasst. Die deutsche Übersetzung erfolgte durch Fujitsu.

Weitere Informationen finden Sie unter: www.fujitsu.com/de/products/computing/storage/data-protection/.

NUTZUNGSHINWEISE

Copyright 2018 Freeform Dynamics Ltd. Dieses Dokument kann in elektronischer oder gedruckter Form frei vervielfältigt und als Ganzes verteilt werden. Es darf jedoch im Rahmen des Vervielfältigungsprozesses nicht aufgeteilt oder modifiziert werden. Das Anbieten des gesamten Berichts zum Download und/oder zur Massenverteilung ist verboten, es sei denn, es liegt eine ausdrückliche Genehmigung von Freeform Dynamics oder Fujitsu vor. Die Inhalte dieses Dokuments dienen nur zur allgemeinen Information und Nutzung, weder Freeform Dynamics noch Dritte garantieren deren Eignung für bestimmte Zwecke.