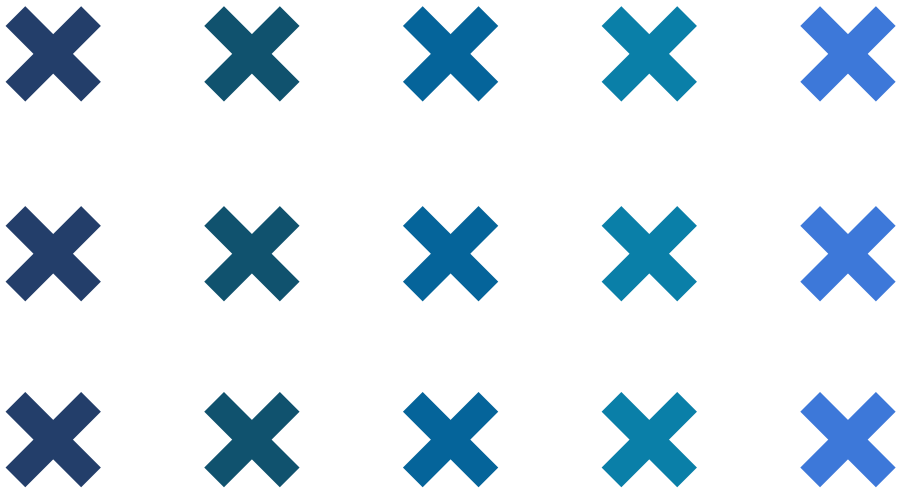
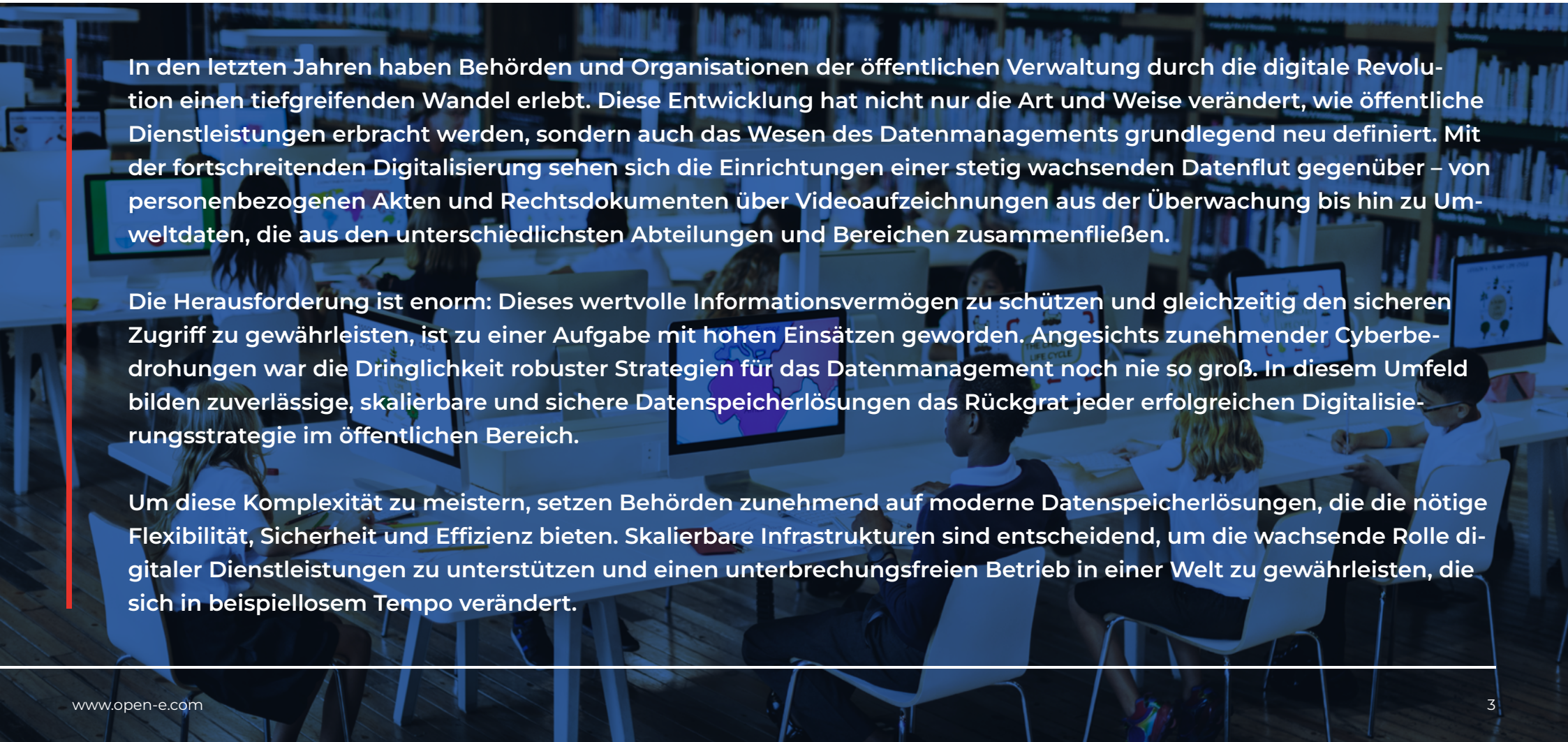

open-e
DATENSPEICHERUNG FÜR
BEHÖRDEN
& VERWALTUNG
mit Open-E JovianDSS

Inhaltsverzeichnis



Digitale Transformation
bei Behörden & Verwaltung



In den letzten Jahren haben Behörden und Organisationen der öffentlichen Verwaltung durch die digitale Revolution einen tiefgreifenden Wandel erlebt. Diese Entwicklung hat nicht nur die Art und Weise verändert, wie öffentliche Dienstleistungen erbracht werden, sondern auch das Wesen des Datenmanagements grundlegend neu definiert. Mit der fortschreitenden Digitalisierung sehen sich die Einrichtungen einer stetig wachsenden Datenflut gegenüber – von personenbezogenen Akten und Rechtsdokumenten über Videoaufzeichnungen aus der Überwachung bis hin zu Umweltdaten, die aus den unterschiedlichsten Abteilungen und Bereichen zusammenfließen.

Die Herausforderung ist enorm: Dieses wertvolle Informationsvermögen zu schützen und gleichzeitig den sicheren Zugriff zu gewährleisten, ist zu einer Aufgabe mit hohen Einsätzen geworden. Angesichts zunehmender Cyberbedrohungen war die Dringlichkeit robuster Strategien für das Datenmanagement noch nie so groß. In diesem Umfeld bilden zuverlässige, skalierbare und sichere Datenspeicherlösungen das Rückgrat jeder erfolgreichen Digitalisierungsstrategie im öffentlichen Bereich.

Um diese Komplexität zu meistern, setzen Behörden zunehmend auf moderne Datenspeicherlösungen, die die nötige Flexibilität, Sicherheit und Effizienz bieten. Skalierbare Infrastrukturen sind entscheidend, um die wachsende Rolle digitaler Dienstleistungen zu unterstützen und einen unterbrechungsfreien Betrieb in einer Welt zu gewährleisten, die sich in beispiellosem Tempo verändert.

Statistiken zur Datenspeicherung bei Behörden & Verwaltung

Hier einige Statistiken zu Digitalisierungsaspekten und zur Datenspeichernutzung bei Behörden & Verwaltung:

Ransomware-Angriffsquoten in den USA

(Staatliche und kommunale Behörden, die von Ransomware betroffen sind)

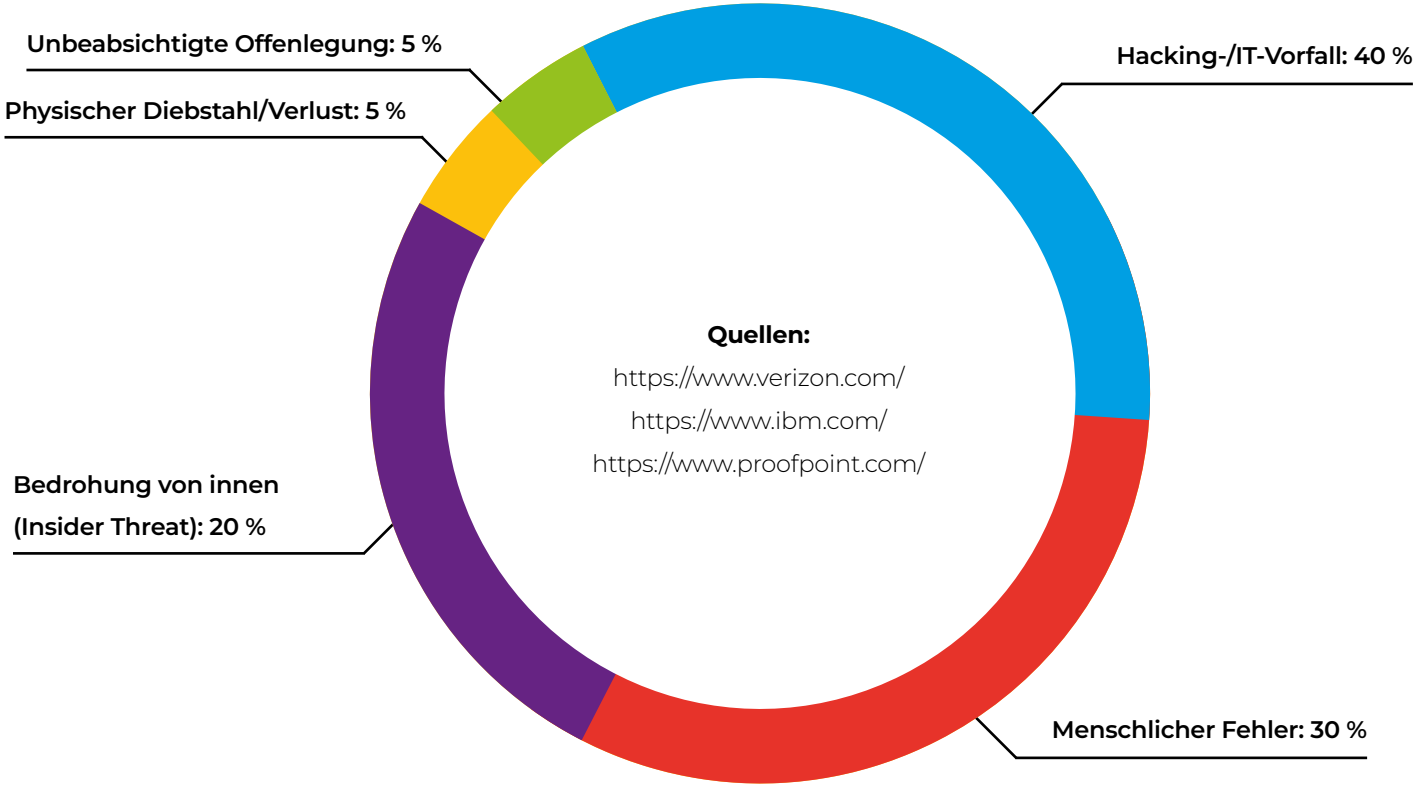
Weltweite Wiederherstellungskosten

(Durchschnittliche Kosten zur Behebung eines Ransomware-Angriffs)

Cyberbedrohungen im öffentlichen Sektor

- **2023:** 15 % aller erfolgreichen Angriffe auf Organisationen im öffentlichen Sektor wurden mit Malware durchgeführt, darunter auch Remote-Access-Trojaner und Spyware – die häufigste Angriffsmethode.
- **2024:** 68 % der erfolgreichen Angriffe auf Behörden in der ersten Jahreshälfte wurden mit Malware ausgeführt. Auch der Einsatz fortgeschrittener Bedrohungen wie APT-Gruppen und Methoden zum Abgreifen von Zugangsdaten hält an.

Arten von Datenspeicher-Vorfällen



Aufstieg der Digitalisierung bei Behörden & Verwaltung

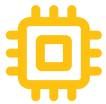
Während die Welt digitale Technologien in rasantem Tempo annimmt, stehen Behörden und öffentliche Organisationen an einem Wendepunkt. Die dringende Umstellung auf digitalisierte Umgebungen macht nicht nur die Notwendigkeit moderner IT-Infrastrukturen deutlich, sondern unterstreicht auch den kritischen Bedarf an effizientem Datenmanagement und robusten Sicherheitsmaßnahmen. In diesem sich wandelnden Umfeld ist Digitalisierung nicht nur ein Trend – sie ist der Schlüssel, um die Servicequalität zu verbessern und Transparenz in der öffentlichen Verwaltung zu fördern.

Steigende Nachfrage nach Online-Diensten

Bürger und Unternehmen erwarten heute schnellen, reibungslosen und sicheren Online-Zugang zu Verwaltungsleistungen. Von Steuererklärungen und öffentlichen Registern bis hin zu Gesundheitsdiensten und juristischen Verfahren. Digitale Plattformen sind unverzichtbar für eine effiziente öffentliche Leistungserbringung geworden. Diese Nachfrage nach jederzeit verfügbaren und sicheren Diensten zwingt Behörden, ihre IT-Infrastruktur zu modernisieren, um sicherzustellen, dass Daten jederzeit verfügbar, geschützt und effizient verwaltet werden.

Pandemiebedingte Veränderungen

Die COVID-19-Pandemie hat die digitale Transformation in allen Bereichen – auch in der öffentlichen Verwaltung – stark beschleunigt. Lockdowns und Abstandsregelungen machten es unmöglich, sich ausschließlich auf physische Vor-Ort-Dienste zu verlassen. Weltweit mussten Verwaltungen schnell auf Online-Modelle umstellen, um Mitarbeitenden die Arbeit aus der Ferne und Bürgern den digitalen Zugang zu Dienstleistungen zu ermöglichen. Dieser Wandel führte zu einem sprunghaften Anstieg des erzeugten, geteilten und gespeicherten Datenvolumens – wodurch robuste, skalierbare Datenspeicherlösungen wichtiger wurden als je zuvor.

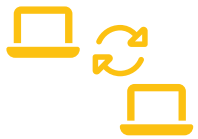


Die Notwendigkeit moderner Infrastrukturen

Mit der fortschreitenden Digitalisierung können veraltete Systeme den Anforderungen des modernen Datenmanagements nicht mehr gerecht werden. Ältere Datenspeicherlösungen sind oft ineffizient, schwer skalierbar und verfügen nicht über die Sicherheitsmaßnahmen, die zum Schutz vor heutigen Cyberbedrohungen erforderlich sind. Die Modernisierung der Infrastruktur, insbesondere im Bereich der Datenspeicherung ist für Behörden zu einer Priorität geworden, um die betriebliche Effizienz zu steigern, Kosten zu senken und die Qualität öffentlicher Dienstleistungen zu verbessern.

Auswirkungen der Digitalisierung auf Behörden & Verwaltung

Die Digitalisierung hat die Arbeitsweise von Behörden und Organisationen der öffentlichen Verwaltung grundlegend verändert. Durch die Ablösung papierbasierter Prozesse durch elektronische Systeme wurden Arbeitsabläufe erheblich verbessert, Daten leichter zugänglich gemacht und die Transparenz öffentlicher Dienstleistungen gesteigert.



Optimierte Arbeitsabläufe

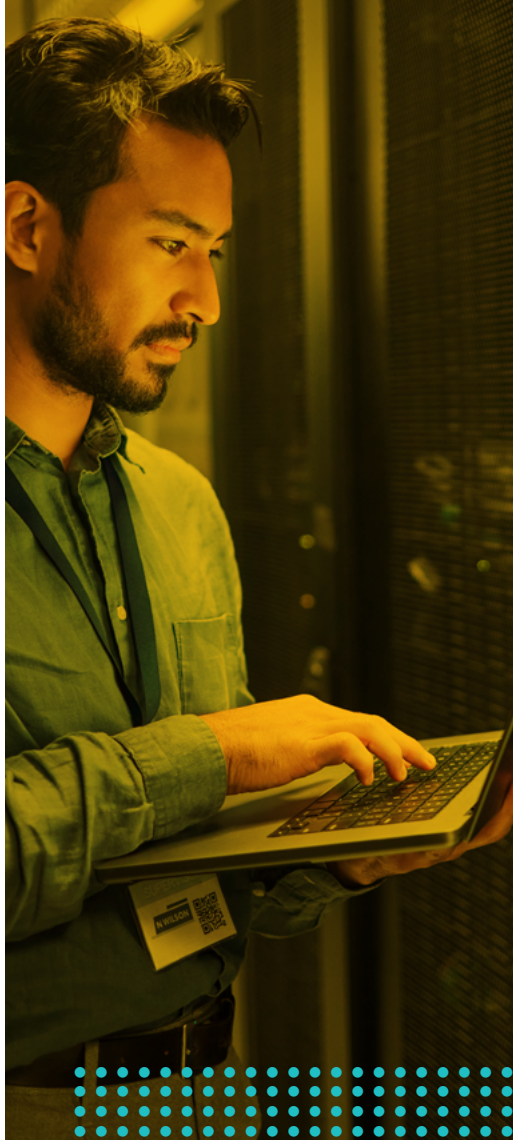
Die Digitalisierung vereinfacht komplexe Verwaltungsprozesse, die zuvor auf manueller Dokumentenbearbeitung und persönlichen Interaktionen beruhten. Mit digitalen Systemen werden Aufgaben wie die Bearbeitung von Anträgen, Verwaltung von Bürgerakten oder Ausstellung von Lizenzen automatisiert. Das reduziert den Zeit- und Arbeitsaufwand erheblich, beschleunigt die Servicebereitstellung, verringert Fehler und ermöglicht eine effizientere Ressourcennutzung.

Verbesserte Zugänglichkeit

Bürgerinnen und Bürger können öffentliche Dienstleistungen nun jederzeit und von überall online in Anspruch nehmen. Ob Steuerzahlung, Führerscheinverlängerung, Antragstellung oder Zugang zu Gesundheitsdiensten, digitale Plattformen haben die Verwaltung für die Öffentlichkeit deutlich zugänglicher gemacht. Diese gesteigerte Erreichbarkeit ist besonders für Menschen in abgelegenen Regionen oder mit eingeschränkter Mobilität von Vorteil, da sie ohne physische Barrieren mit der Verwaltung interagieren können.

Mehr Transparenz

Die Digitalisierung steigert zudem die Transparenz, indem Bürger den Fortschritt ihrer Anträge verfolgen, auf öffentliche Daten zugreifen und einfacher an Verwaltungsprozessen teilnehmen können. Digitale Aufzeichnungen und Datenbanken schaffen klare Prüfpfade, gewährleisten Rechenschaftspflicht und verringern Möglichkeiten für Korruption oder Fehler. Das fördert das Vertrauen zwischen Verwaltung und Bevölkerung nachhaltig.



Verbesserte Gesetzgebung, Regulierung und Sicherheit

Gut strukturierte und leicht zugängliche Datenspeicherung unterstützt die Einhaltung gesetzlicher Vorschriften und die öffentliche Sicherheit, indem Beweise und Dokumentationen erhalten bleiben. Die Analyse gespeicherter Daten kann dabei helfen, Bereiche zu identifizieren, in denen neue Gesetze erforderlich sind oder bestehende angepasst werden sollten. So können beispielsweise Daten aus den Bereichen öffentliche Sicherheit, Verkehr und Katastrophenschutz genutzt werden, um Aktualisierungen von Sicherheitsvorschriften zu steuern und so das Wohlbefinden sowie die Sicherheit der Gemeinschaft zu fördern.

Datenanalyse

Mit leistungsstarken Datenspeicherlösungen können Institutionen große Mengen historischer und aktueller Echtzeitdaten effizient erfassen und vorhalten. Dies ermöglicht eine tiefgehende Analyse von Trends, Mustern und Zusammenhängen. Auf dieser Grundlage lassen sich fundierte, datengestützte Entscheidungen in Bereichen wie öffentliche Gesundheit, Kriminalitätsbekämpfung und Ressourcenverteilung treffen. Dazu werden Erkenntnisse aus Kriminalitätsstatistiken, Gesundheitsakten oder Wirtschaftsdaten genutzt. Der Zugriff auf gut organisierte und aktuelle Daten versetzt Verwaltungen in die Lage, schnell auf Herausforderungen zu reagieren – von der Festlegung gesundheitspolitischer Maßnahmen bis hin zur Optimierung des Katastrophenschutzes – und so Dienstleistungen zu verbessern und Ressourcen gezielt einzusetzen.

Bessere Einblicke in gesellschaftliche Probleme

Zuverlässige und skalierbare Datenspeicherung erleichtert die Zusammenführung umfangreicher Datensätze aus verschiedenen Quellen wie Polizei, Gesundheitswesen, Bildung und öffentlichen Diensten. Die Analyse dieser Daten hilft Verwaltungen, komplexe gesellschaftliche Probleme wie Armut, Kriminalität oder Bildungsdefizite besser zu verstehen. Mit tieferem Verständnis der Ursachen und Zusammenhänge können Regierungen wirksamere Strategien und Maßnahmen entwickeln und umsetzen.

Zentrale Herausforderungen der Datenspeicherung bei Behörden & Verwaltung

Wenn Behörden und Organisationen der öffentlichen Verwaltung ihre digitale Transformation vorantreiben, sehen sie sich einer Reihe erheblicher Herausforderungen bei der Datenspeicherung gegenüber, die ihre Fähigkeit zur Erbringung wesentlicher Dienstleistungen gefährden können. Man stelle sich eine stark ausgelastete Behörde vor, die riesige Datenmengen verwaltet – von personenbezogenen Akten bis hin zu wichtigen öffentlichen Informationen – und gleichzeitig sensible Daten vor sich ständig weiterentwickelnden Cyberbedrohungen schützen muss. In diesem sensiblen Umfeld sind Kosteneffizienz und die Sicherstellung der Betriebskontinuität von höchster Bedeutung. Ohne robuste, skalierbare und sichere Speicherlösungen riskieren diese Institutionen, ihren Auftrag nicht vollständig zu erfüllen. Die erfolgreiche Bewältigung dieser Herausforderungen dient nicht nur der Effizienzsteigerung, sondern ist auch entscheidend, um das Vertrauen der Öffentlichkeit zu gewinnen und die Einhaltung strenger gesetzlicher Vorschriften sicherzustellen.

Schutz vor Angriffen auf Wahlprozesse

Um Wahlprozesse vor Angriffen zu schützen, setzen Speichersysteme auf Desaster-Recovery- und Datenreplikationsfunktionen. Bei Ransomware- oder DDoS-Angriffen minimieren diese Systeme Ausfallzeiten und ermöglichen eine schnelle Wiederherstellung aus sicheren Backups, um den Betrieb aufrechtzuerhalten. Die Replikation von Daten über mehrere Standorte hinweg stellt sicher, dass wahlrelevante Informationen auch dann verfügbar bleiben, wenn ein primäres Rechenzentrum kompromittiert ist, und unterstützt so kontinuierliche Wahlabläufe in kritischen Situationen. Die Einhaltung von Sicherheitsstandards wie FISMA und FedRAMP bietet zudem eine zusätzliche Schutzebene gegen Cyberangriffe.

Bekämpfung von Desinformation

Eine effektive Datenspeicherung trägt auch dazu bei, die Verbreitung von Desinformation in Behörden und Verwaltung zu verhindern. Lösungen mit robuster Metadatenverfolgung verifizieren Datenquellen und unterstützen so die Authentizität der innerhalb von Behörden geteilten Informationen, was die Ausbreitung falscher Inhalte reduziert. Fortschrittliche Speichersysteme mit KI-gestützter Analyse können Datenmuster überwachen, um abnormale Inhalte zu erkennen und zu entschärfen, die mit Desinformationskampagnen in Verbindung stehen. Darüber hinaus schützen strenge Datenschutzprotokolle und klar strukturierte Datenbereiche sensible Informationen vor unbefugtem Zugriff und verringern so das Risiko von Leaks oder Manipulationen, die Desinformation begünstigen könnten.

Mehr Transparenz und öffentliches Vertrauen

Sichere Datenspeicherung steigert die Transparenz und stärkt das Vertrauen der Öffentlichkeit. Speicherlösungen, die öffentliche Datenfreigabeplattformen unterstützen, ermöglichen in Echtzeit den Zugriff auf verifizierte und korrekte Informationen, wie zum Beispiel geprüfte Wahlergebnisse. Dies schränkt die Wirksamkeit irreführender Narrative ein. Blockchain- oder unveränderliche Speicherverfahren erhöhen die Transparenz zusätzlich, indem sie eine manipulationssichere Historie aller Dateninteraktionen bereitstellen und so das Vertrauen in die Authentizität behördlicher Aufzeichnungen fördern. Zusammen gewährleisten diese Speichermaßnahmen eine hohe Zuverlässigkeit, Sicherheit und Verfügbarkeit von Daten, was für den Schutz vor äußerer Einflussnahme und Desinformation im öffentlichen Sektor unerlässlich ist.

Speicherung großer Datenmengen

Behörden und öffentliche Organisationen müssen enorme Datenmengen verwalten, darunter Bürgerakten, Rechtsdokumente und digitale Dienste. Hierfür werden skalierbare Speicherlösungen benötigt, die Wachstum unterstützen und gesetzliche Vorgaben einhalten. Gleichzeitig müssen sensible Informationen wie personenbezogene Daten oder vertrauliche Dokumente vor Cyberbedrohungen und Sicherheitsverletzungen geschützt werden. Dazu sind robuste Verschlüsselung, Zugriffskontrollen und kontinuierliche Sicherheitsüberwachung unverzichtbar. Zunehmende Ransomware-Gefahren und die wachsende Bedeutung der Datensouveränität verschärfen diese Anforderungen zusätzlich.

Kosteneffizienz erreichen

Öffentliche Einrichtungen arbeiten häufig mit begrenzten Budgets und benötigen daher Speicherlösungen, die Kostenersparnis mit hoher Leistung, Sicherheit und Skalierbarkeit verbinden. Kosteneffizienz kann durch Technologien wie Deduplizierung, Kompression und flexible Hardware-Auswahl erreicht werden, die die Gesamtausgaben senken, ohne die Zuverlässigkeit zu beeinträchtigen.

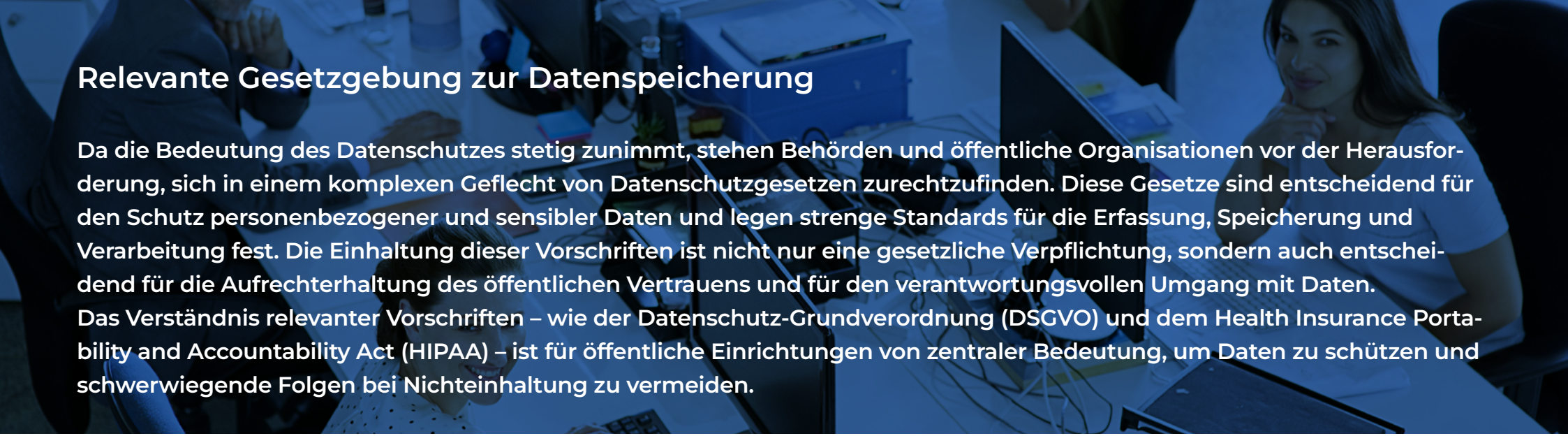
Betriebskontinuität und Desaster-Recovery sicherstellen

Öffentliche Dienste erfordern durchgehende Verfügbarkeit und verlässlichen Datenzugriff. Jede Unterbrechung – ob durch Cyberangriffe, Naturkatastrophen oder Systemausfälle – kann schwerwiegende Folgen haben. Um Kontinuität zu gewährleisten, sind fortschrittliche Desaster-Recovery-Pläne, Hochverfügbarkeitskonfigurationen sowie automatisierte, regelmäßige Backups notwendig, um Ausfallzeiten zu minimieren und eine schnelle Datenwiederherstellung sicherzustellen.

Datenmanagement bei Behörden & Verwaltung

Die Sicherheit der Datenspeicherung geht in Behörden und öffentlichen Einrichtungen weit über die reine Einhaltung gesetzlicher Vorschriften hinaus und ist ein Grundpfeiler des öffentlichen Vertrauens. Diese Organisationen verwalten eine enorme Bandbreite sensibler Informationen, darunter personenbezogene Akten, Gesundheitsdaten und sicherheitsrelevante Details auf nationaler Ebene. Die Verantwortung für den Schutz dieser Daten lastet schwer auf den Verantwortlichen, da ihre Entscheidungen nicht nur die Sicherheit gewährleisten müssen, sondern auch im Einklang mit einem komplexen Geflecht nationaler und internationaler Vorschriften stehen müssen.

Im Folgenden betrachten wir die wesentlichen Sicherheitsanforderungen und gesetzlichen Regelungen, die die Datenspeicherung im öffentlichen Sektor bestimmen. Dabei wird deutlich, welche entscheidenden Maßnahmen diese Institutionen ergreifen, um Transparenz und Rechenschaftspflicht in ihren Datenmanagementprozessen sicherzustellen.



Relevante Gesetzgebung zur Datenspeicherung

Da die Bedeutung des Datenschutzes stetig zunimmt, stehen Behörden und öffentliche Organisationen vor der Herausforderung, sich in einem komplexen Geflecht von Datenschutzgesetzen zurechtzufinden. Diese Gesetze sind entscheidend für den Schutz personenbezogener und sensibler Daten und legen strenge Standards für die Erfassung, Speicherung und Verarbeitung fest. Die Einhaltung dieser Vorschriften ist nicht nur eine gesetzliche Verpflichtung, sondern auch entscheidend für die Aufrechterhaltung des öffentlichen Vertrauens und für den verantwortungsvollen Umgang mit Daten.
Das Verständnis relevanter Vorschriften – wie der Datenschutz-Grundverordnung (DSGVO) und dem Health Insurance Portability and Accountability Act (HIPAA) – ist für öffentliche Einrichtungen von zentraler Bedeutung, um Daten zu schützen und schwerwiegende Folgen bei Nichteinhaltung zu vermeiden.

§ Datenschutz-Grundverordnung (DSGVO) – Europäische Union

Die DSGVO ist eines der weltweit umfassendsten Datenschutzgesetze und regelt, wie personenbezogene Daten erfasst, gespeichert und verarbeitet werden. Behörden und öffentliche Einrichtungen in der EU müssen die Vorgaben der DSGVO erfüllen. Dazu gehören unter anderem die sichere Speicherung personenbezogener Daten, der Einsatz von Verschlüsselung sowie die Meldung von Datenschutzverletzungen innerhalb strenger Fristen. Verstöße können zu erheblichen Geldbußen führen.

§ Health Insurance Portability and Accountability Act (HIPAA) – Vereinigte Staaten

Obwohl HIPAA in erster Linie für Organisationen im Gesundheitswesen gilt, ist es auch für öffentliche Gesundheitsbehörden und staatliche Stellen relevant, die Gesundheitsdienste erbringen. HIPAA schreibt strenge Sicherheitsmaßnahmen zum Schutz sensibler Gesundheitsdaten vor, darunter sichere Speicherung, Verschlüsselung, Zugriffskontrolle und regelmäßige Überprüfung der Datenverarbeitungspraktiken.

§ Federal Information Security Management Act (FISMA) – Vereinigte Staaten

FISMA verpflichtet US-Bundesbehörden, umfassende Programme zur Informationssicherheit zu implementieren, um staatliche Informationssysteme zu schützen. Dazu gehören Sicherheitsmaßnahmen wie Datenverschlüsselung, Eindringungserkennung, kontinuierliche Überwachung und regelmäßige Risikobewertungen, um die Einhaltung von Bundesstandards wie den NIST-SP-800-53-Richtlinien sicherzustellen.

§ Public Services Network (PSN) Compliance – Vereinigtes Königreich

Das PSN ist ein Regierungsnetzwerk, das einen sicheren Datenaustausch zwischen Organisationen des öffentlichen Sektors im Vereinigten Königreich ermöglicht. Für die Nutzung des PSN müssen Organisationen strenge Sicherheitsprotokolle einhalten, darunter die sichere Speicherung von Daten, Verschlüsselung und robuste Zugriffskontrollen. Jährliche Compliance-Prüfungen sind vorgeschrieben, um die fortlaufende Einhaltung der Sicherheitsstandards sicherzustellen.

§ Cloud Act – Vereinigte Staaten

Der CLOUD Act (Clarifying Lawful Overseas Use of Data) verpflichtet US-Technologieunternehmen, Strafverfolgungsbehörden Daten bereitzustellen, die auf ihren Servern gespeichert sind – auch wenn sich diese im Ausland befinden. Dieses Gesetz beeinflusst, wie Anbieter von Datenspeicherlösungen Anfragen von Regierungsstellen bearbeiten, insbesondere in Cloud-Umgebungen. Behörden müssen bei der Datenspeicherung berücksichtigen, wo ihre Daten liegen und wie diese von internationalen Gesetzen betroffen sein könnten.

§ Nationale Datenschutzgesetze und Anforderungen an die nationale Sicherheit

Viele Länder verfügen über eigene Datenschutzgesetze und Vorschriften zur nationalen Sicherheit, die regeln, wie Regierungsdaten gespeichert und geschützt werden müssen. Beispiele sind das Bundesdatenschutzgesetz (BDSG) in Deutschland oder die Vorschriften der CNIL in Frankreich, die strenge Regeln für den Umgang mit personenbezogenen Daten in öffentlichen Einrichtungen vorschreiben. Diese Gesetze enthalten häufig Vorgaben zu Verschlüsselung, Datenaufbewahrung und Meldepflichten bei Datenschutzverletzungen.

§ Richtlinie zu Netz- und Informationssystemen (NIS-2) – Europäische Union

Die NIS-2-Richtlinie verschärft die Cybersicherheitsstandards in wichtigen Sektoren, darunter Behörden und öffentliche Dienste, um die Widerstandsfähigkeit von Informationssystemen zu gewährleisten. Sie schreibt Maßnahmen zum Risikomanagement, schnelle Vorfallsmeldungen innerhalb von 24 Stunden sowie sichere Protokolle zur Datenspeicherung wie Verschlüsselung und Zugriffskontrolle vor. Zudem erweitert sie ihren Anwendungsbereich auf weitere Einrichtungen, mit strenger Compliance und hohen Strafen bei Verstößen, was die Notwendigkeit robuster Cybersicherheitspraktiken unterstreicht.

Wichtige Sicherheitsanforderungen für die Datenspeicherung

In Behörden und öffentlichen Einrichtungen ist die Sicherheit der Datenspeicherung entscheidend, um das Vertrauen der Bevölkerung zu erhalten. Diese Organisationen verwalten sensible Informationen wie personenbezogene Akten, Gesundheitsdaten und sicherheitsrelevante Details, weshalb ein sicheres Management unerlässlich ist. Sie müssen diese Daten nicht nur schützen, sondern auch komplexe gesetzliche Vorschriften einhalten. Im Folgenden werden zentrale Sicherheitsmaßnahmen und rechtliche Rahmenbedingungen erläutert, mit denen Institutionen Transparenz und Rechenschaftspflicht sicherstellen und gleichzeitig wertvolle Informationen schützen.

→ Zugriffskontrolle und Identitätsmanagement

Strenge Zugriffskontrollmechanismen sind entscheidend, um sicherzustellen, dass nur autorisierte Personen auf sensible Daten zugreifen können. Rollenbasierte Zugriffskontrolle (RBAC) und Multi-Faktor-Authentifizierung (MFA) helfen, den Zugriff auf vertrauliche Informationen zu beschränken. Detaillierte Protokollierung und Überwachung von Zugriffsaktivitäten sind zudem erforderlich, um mögliche Sicherheitsverletzungen nachzuvollziehen und zu verhindern.

→ Datenintegrität

Die Gewährleistung der Datenintegrität ist entscheidend, da Korruption oder Manipulation von Datensätzen zu gravierenden Folgen in der Verwaltung führen können. Technologien wie Daten-Checksummen, Fehlererkennung und automatische Datenreparaturmechanismen (z. B. in ZFS-basierten Systemen wie Open-E JovianDSS) tragen dazu bei, Datenkorruption zu verhindern.

→ Backup und Desaster-Recovery

Behörden müssen umfassende Backup-Strategien und Pläne für die Wiederherstellung nach Katastrophen implementieren. Dazu gehören regelmäßige, automatisierte Backups vor Ort und extern, um Datenverluste durch Cyberangriffe, Naturkatastrophen oder menschliche Fehler zu minimieren. Oft schreiben staatliche Standards vor, dass Daten im Notfall schnell wiederhergestellt werden können.

→ Datenverschlüsselung

Verschlüsselung ist eine grundlegende Anforderung zum Schutz sensibler Regierungsdaten, sowohl im Ruhezustand als auch bei der Übertragung. So bleibt sichergestellt, dass Daten ohne die richtigen Entschlüsselungsschlüssel unlesbar und unbrauchbar sind, selbst wenn ein unbefugter Zugriff erfolgt. Behörden müssen häufig starke Verschlüsselungsstandards einsetzen, um Informationen wirksam zu sichern.

→ Schutz vor Ransomware

Regierungen sind häufig Ziel von Ransomware-Angriffen, die essenzielle Dienste stören und sensible Daten gefährden können. Schutzstrategien umfassen die Erstellung unveränderlicher Backups, regelmäßige Software-Updates zur Schließung von Sicherheitslücken und den Einsatz von Eindringungserkennungssystemen, die Administratoren bei verdächtigen Aktivitäten alarmieren.

Sichere Datenspeicherung für Behörden & Verwaltung mit Open-E JovianDSS

Die vertrauenswürdige Lösung für 2025 und darüber hinaus

Vertrauenswürdige Lösung für 2025 und die Zukunft

Schützen Sie Ihre Behördendaten mit Open-E JovianDSS. Diese hochmoderne Speichertechnologie erfüllt strenge gesetzliche Anforderungen, bietet optimiertes, skalierbares und geschütztes Datenmanagement – ohne Herstellerbindung und zu geringeren Kosten.

Wahrung der Integrität nationaler und öffentlicher Daten

Schützen Sie geschäftskritische Informationen in Behörden, Justiz und Verteidigung. Open-E JovianDSS gewährleistet Sicherheit, nahtlose Skalierbarkeit und bereitet Ihre Infrastruktur auf die Zukunft vor.

Warum Führungskräfte in Behörden & Verwaltung Open-E JovianDSS wählen:

- **Compliance-fähige Verschlüsselung**
  Mit Self-Encrypting Drives (SEDs) schützt Open-E JovianDSS sensible Behördendaten und erfüllt strengste Datenschutz- und Datensicherheitsstandards.
- **Zuverlässige Betriebskontinuität & Desaster-Recovery**
  Stillstand ist keine Option. Open-E JovianDSS bietet Hochverfügbarkeits-Cluster sowie On- & Off-Site-Datenschutz, um den Datenzugriff selbst bei Cyberangriffen oder Systemausfällen sicherzustellen.
- **Nahtlose Skalierbarkeit für wachsende Speicheranforderungen**
  Die hardware- und hypervisorunabhängige Architektur von Open-E JovianDSS ermöglicht die flexible Erweiterung Ihrer Infrastruktur bei steigenden Anforderungen – mit maximaler Flexibilität und Leistung.
- **Snapshot-Technologie als Schutz vor Cyberangriffsfolgen**
  Erstellen Sie sofort schreibgeschützte Snapshots Ihrer Datenspeicher. Im Falle eines Ransomware-Angriffs können Sie einfach auf einen sauberen Stand zurückkehren – kein Lösegeld, keine Ausfallzeit.
- **Kosteneffiziente Speicheroptimierung**
  Sparen Sie Kosten, ohne Leistung oder Sicherheit zu beeinträchtigen. Nutzen Sie Speichereffizienz-Funktionen wie Deduplizierung und individuell anpassbare Aufbewahrungspläne.

Erfahren Sie, wie **Open-E JovianDSS** Ihre Datensicherheit und Ausfallsicherheit im Behördenumfeld steigert. Scannen Sie den QR-Code oder besuchen Sie **open-e.com**, um mehr zu erfahren und eine Demo zu vereinbaren.

Sichern Sie Ihre Infrastruktur mit der vertrauenswürdigen Wahl für Datenspeicherung im öffentlichen Sektor – Open-E JovianDSS!

Open-E Lösungen für Herausforderungen bei der Datenspeicherung

Wenn Behörden und öffentliche Einrichtungen die digitale Transformation vorantreiben, sehen sie sich wachsenden Herausforderungen bei der Verwaltung und Sicherung großer Datenmengen gegenüber. Die Notwendigkeit zuverlässiger und effizienter Speicherlösungen war noch nie so groß, da diese Institutionen ihre Servicequalität verbessern, die Einhaltung gesetzlicher Vorgaben sicherstellen und sensible Informationen schützen müssen. Mit dem steigenden Bedarf an Zugänglichkeit, Skalierbarkeit und Sicherheit müssen moderne Strategien für das Datenmanagement eingeführt werden, um den sich verändernden Anforderungen gerecht zu werden und gleichzeitig die Betriebskontinuität zu wahren.

So begegnet Open-E JovianDSS diesen Herausforderungen:
Open-E JovianDSS bietet maßgeschneiderte Speicherlösungen, die Datenintegrität und Zugänglichkeit priorisieren und es Behörden ermöglichen, die Komplexität des digitalen Datenmanagements effizient zu bewältigen. Durch die Implementierung dieser Lösungen können öffentliche Einrichtungen nicht nur sensible Daten schützen, sondern auch Arbeitsabläufe optimieren und so schneller und gezielter auf die Bedürfnisse von Bürgerinnen und Bürgern reagieren.

Compliance und Datensouveränität

Open-E JovianDSS gewährleistet die Einhaltung globaler und nationaler Datenschutzgesetze. Das System unterstützt Festplattenverschlüsselung, Zugriffskontrollen und sichere Datenreplikation und ermöglicht es Institutionen, die Anforderungen an die Datensouveränität zu erfüllen, indem sensible Daten ausschließlich innerhalb nationaler Grenzen oder definierter geografischer Standorte gespeichert werden.

- **Anwendungsbeispiel aus Behörden & Verwaltung**
  Eine nationale Regierungsbehörde nutzt Open-E JovianDSS, um vertrauliche Informationen in einer privaten Cloud-Infrastruktur innerhalb nationaler Grenzen zu speichern und so die Einhaltung der Vorschriften zur Datensouveränität sicherzustellen.

Kosteneffizienz

Open-E JovianDSS ist als kosteneffiziente Speicherlösung für Behörden und öffentliche Einrichtungen konzipiert, um die Ressourcennutzung zu optimieren und die Gesamtbetriebskosten zu senken. Wesentliche Faktoren, die zur Kosteneffizienz beitragen, sind:

- **Virtualisierung:** Durch die Unterstützung verschiedener Virtualisierungsplattformen (z. B. VMware, Microsoft Hyper-V, Proxmox) ermöglicht Open-E JovianDSS die Konsolidierung der IT-Infrastruktur. So können mehrere virtuelle Maschinen auf einem einzelnen physischen Server betrieben werden, was den Bedarf an umfangreichen Hardwareinvestitionen reduziert. Gleichzeitig wird die Ressourcenzuweisung vereinfacht, sodass die Infrastruktur bedarfsgerecht skaliert werden kann, ohne erhebliche Zusatzkosten zu verursachen.
- **Hypervisor-Unabhängigkeit:** Open-E JovianDSS ist hypervisorunabhängig und lässt sich nahtlos mit jeder Virtualisierungsplattform integrieren. Behörden können so den Hypervisor auswählen, der ihren Anforderungen am besten entspricht, ohne an das Ökosystem eines bestimmten Herstellers gebunden zu sein. Dies optimiert die Ressourcennutzung, senkt Kosten und ermöglicht die Nutzung bestehender Virtualisierungsinvestitionen.
- **Hardware-Unabhängigkeit:** Die hardwareunabhängige Architektur ermöglicht den Einsatz einer breiten Palette von Hardwarekonfigurationen – von Standard-x86-Servern bis zu spezialisierten Speichergeräten. So können bestehende Hardware genutzt oder kostengünstige Optionen gewählt werden, die zum Budget passen. Proprietäre Hardwarevorgaben werden vermieden, was die Lebensdauer der Assets verlängert und wettbewerbsfähige Preise ermöglicht.

Anwendungsbeispiel aus Behörden & Verwaltung

Eine Stadtverwaltung kann mit Open-E JovianDSS ein virtualisiertes Rechenzentrum aufbauen, um Hardware- und Energiekosten zu senken. Die hypervisor- und hardwareunabhängigen Funktionen ermöglichen eine flexible Anpassung der Infrastruktur, optimale Ressourcennutzung und vermeiden Herstellerabhängigkeiten.

Skalierbarkeit

Open-E JovianDSS verwendet das ZFS-Dateisystem, das für die Verwaltung großer Datenmengen ausgelegt ist. Es bietet nahezu unbegrenzte Skalierbarkeit, sodass Institutionen enorme Datenbestände ohne Leistungseinbußen speichern können. Die Speicherkapazität lässt sich jederzeit durch das Hinzufügen neuer Festplatten erweitern, ohne den laufenden Betrieb zu unterbrechen – ideal für Einrichtungen mit stetig wachsendem Datenvolumen.

Anwendungsbeispiel aus Behörden & Verwaltung

Ein nationales Archiv kann mit Open-E JovianDSS jahrzehntelange Datenbestände – von Geburtsurkunden und Steuerunterlagen bis hin zu Umweltdaten – verwalten und dabei schnellen Zugriff sowie Aktualisierungen in Echtzeit sicherstellen, ohne die Infrastruktur ständig aufrüsten zu müssen.

Datensicherheit und -integrität

Open-E JovianDSS wurde entwickelt, um umfassenden, unternehmenskritischen Schutz für sensible und missionskritische Informationen zu bieten. Es erfüllt die hohen Anforderungen an Sicherheit und Integrität in Behörden und öffentlichen Einrichtungen, indem es eine skalierbare und hochverfügbare Speicherlösung bereitstellt. Die Lösung ist auf strikte Compliance- und regulatorische Vorgaben ausgelegt und ermöglicht die sichere Speicherung großer Datenmengen bei gleichzeitig eingeschränktem, aber kontinuierlichem Zugriff und hoher Performance.

- **SEDs:** Unterstützung von selbstverschlüsselnden Festplatten (Self-Encrypting Drives) stellt sicher, dass Daten im Ruhezustand geschützt sind und strenge gesetzliche Standards erfüllt werden.
- **ZFS-Technologie:** End-to-End-Checksumming erkennt und behebt automatisch Datenkorruption, um die Integrität kritischer Datensätze zu gewährleisten.
- **RBAC:** Rollenbasierte Zugriffskontrollen beschränken den Zugriff auf autorisierte Benutzer, während umfassende Protokollierung die Sicherheitsüberwachung und Nachvollziehbarkeit verbessert.
- **Open-E Hochverfügbarkeits-Cluster und On- & Off-Site-Datenschutz:** Diese Funktionen ermöglichen öffentlichen Einrichtungen den kontinuierlichen Zugriff auf wichtige Informationen sowie zuverlässige Wiederherstellungslösungen und unterstreichen ihr Engagement für Datensicherheit in einer dynamischen digitalen Umgebung.

✓ **Anwendungsbeispiel aus Behörden & Verwaltung**

Gesundheitsämter speichern und verwalten sensible medizinische Daten verschlüsselt, um sicherzustellen, dass Patientendaten sicher und unverändert bleiben und die Datenschutzanforderungen wie HIPAA erfüllt werden.

Snapshots und Aufbewahrungspläne

- **Snapshots:** Snapshots in ZFS sind schreibgeschützte Kopien des Dateisystems zu einem bestimmten Zeitpunkt. Sie werden schnell und effizient erstellt und ermöglichen es, den aktuellen Datenstand ohne erheblichen zusätzlichen Speicherplatzbedarf zu sichern. So können Einrichtungen nach versehentlichen Löschungen, Datenkorruption, Ransomware-Angriffen oder anderen Problemen rasch den vorherigen Systemzustand wiederherstellen.
- **Aufbewahrungspläne:** Diese nutzen Snapshots zur Verwaltung des Datenlebenszyklus, indem definiert wird, wie lange Snapshots aufbewahrt werden, bevor sie automatisch gelöscht werden. So wird eine strukturierte Herangehensweise an die Datenaufbewahrung gewährleistet, damit notwendige Informationen für Compliance, Audits oder Wiederherstellungen verfügbar sind. Gleichzeitig werden Speicherkapazitäten effizient genutzt und Risiken durch Datenverlust oder Nichteinhaltung gesetzlicher Vorgaben reduziert.

✓ **Anwendungsbeispiel aus Behörden & Verwaltung**

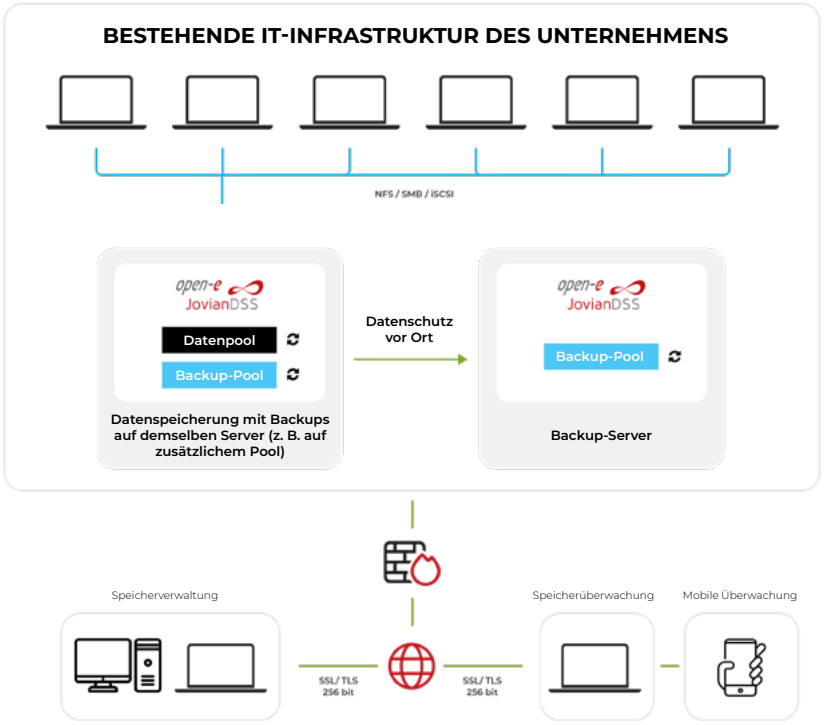
Eine Behörde kann mithilfe von Snapshots regelmäßig schreibgeschützte Kopien sensibler Patientendaten erstellen. Tritt ein Fehler wie eine fehlerhafte Dateneingabe oder ein Cyberangriff auf, kann schnell auf den letzten fehlerfreien Snapshot zurückgegriffen werden, um Ausfallzeiten zu minimieren und sensible Informationen zu schützen.

Eine Behörde im Bereich Umweltüberwachung setzt Aufbewahrungspläne ein, um den Lebenszyklus ihrer Daten zu verwalten. Durch klare Richtlinien, wie lange Snapshots von Umweltdaten aufbewahrt werden, stellt die Behörde die Einhaltung gesetzlicher Vorschriften sicher. So können beispielsweise Snapshots fünf Jahre lang mit entsprechenden Audit-Protokollen gespeichert und ältere Versionen automatisch gelöscht werden. Diese strukturierte Vorgehensweise unterstützt nicht nur die Erfüllung von Compliance- und Forschungsanforderungen, sondern optimiert auch die Speicherkosten durch effizientes Flächenmanagement.

High-Availability-Cluster

Open-E JovianDSS bietet Hochverfügbarkeits-(HA)-Clusterkonfigurationen, bei denen mehrere Speicherknoten zusammenarbeiten, um kontinuierlichen Datenzugriff sicherzustellen. Fällt ein Knoten aus, übernimmt ein anderer nahtlos, wodurch Single Points of Failure vermieden werden. Dies gewährleistet eine durchgehende Betriebsbereitschaft und Dienstverfügbarkeit – ein entscheidender Faktor für kritische Anwendungen im öffentlichen Sektor, bei denen Ausfallzeiten den Betrieb wesentlicher Dienste beeinträchtigen könnten.

- **Anwendungsbeispiel aus Behörden & Verwaltung**
  Städtische Notfalldienste nutzen einen HA-Cluster, um sicherzustellen, dass ihre zentralen Kommunikationssysteme und Datenbanken rund um die Uhr einsatzfähig bleiben, selbst bei schwerwiegenden Hardwareausfällen oder während Wartungsarbeiten.

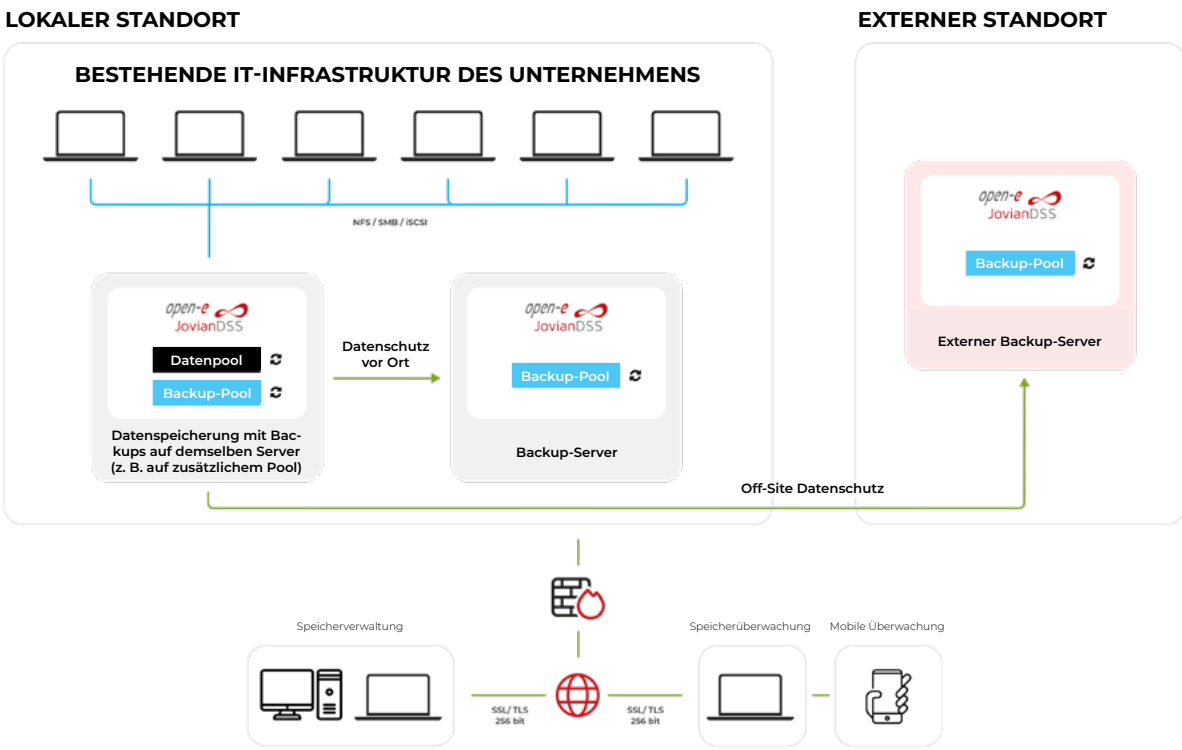


On-Site- und Off-Site-Datensicherung

Open-E JovianDSS unterstützt sowohl lokale (On-Site) als auch externe (Off-Site) Datensicherungen und bietet damit leistungsstarke Lösungen für die Notfallwiederherstellung. Institutionen können regelmäßige lokale Backups planen, um im Bedarfsfall sofortigen Zugriff und eine schnelle Wiederherstellung zu gewährleisten. Zusätzlich kann eine Off-Site-Replikation eingesetzt werden, um Daten vor standortbezogenen Katastrophen wie Bränden, Überschwemmungen oder Cyberangriffen zu schützen. Dies stellt sicher, dass kritische Daten intakt und zugänglich bleiben, selbst wenn das primäre Rechenzentrum kompromittiert wird.

Anwendungsbeispiel aus Behörden & Verwaltung

Eine Verkehrsbehörde repliziert operative Daten an einen externen Standort. Im Falle einer Katastrophe kann die Organisation so wichtige Informationen vom entfernten Standort wiederherstellen und längere Dienstunterbrechungen verhindern.

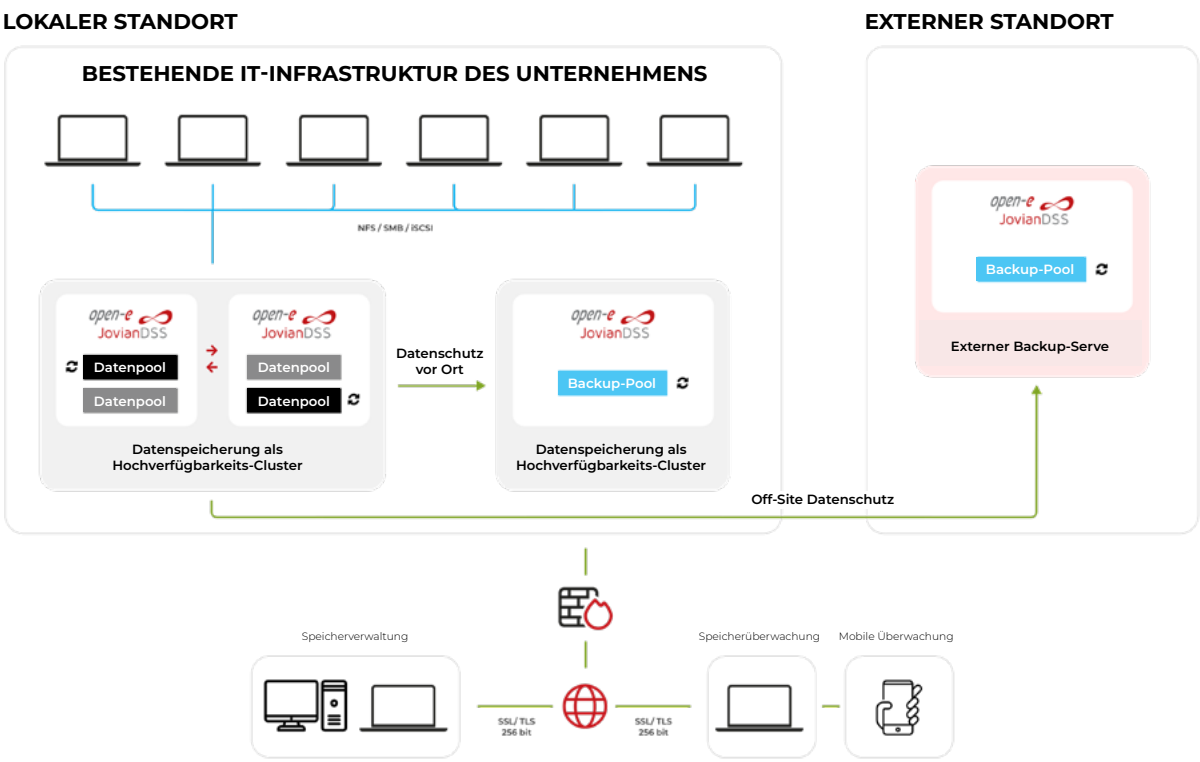


Maximaler Datenschutz

In den Abläufen von Behörden und Verwaltung sind Datensicherheit und ständige Verfügbarkeit nicht verhandelbar, insbesondere bei der Verwaltung kritischer Informationen wie Bürgerakten, sensibler Patientendaten, öffentlicher Sicherheitsdaten und national sicherheitsrelevanter Informationen. Open-E JovianDSS erfüllt diese Anforderungen durch die Kombination von lokaler (On-Site) und externer (Off-Site) Datensicherung mit Hochverfügbarkeits-Clustern.

Dies gewährleistet nahtlosen Datenschutz ohne Beeinträchtigung der Betriebszeit. Diese erweiterte Lösung verbindet schnelle Wiederherstellung durch lokale Backups mit externer Replikation, um Daten vor regionalen Katastrophen wie Bränden, Überschwemmungen oder Cyberangriffen zu schützen. So bleibt sichergestellt, dass wichtige Daten selbst unter extremen Bedingungen zugänglich sind.

- **Anwendungsbeispiel aus Behörden & Verwaltung**
  Gesundheitsbehörden nutzen die Funktionen für maximalen Datenschutz von Open-E JovianDSS, um sensible Patientendaten zu verwalten. Durch regelmäßige Integritätsprüfungen und häufige Snapshots kann die Behörde Daten im Falle versehentlicher Löschungen oder Ransomware-Vorfälle schnell auf einen früheren Zustand zurücksetzen. Dies gewährleistet die Einhaltung von Datenschutzvorschriften und schützt gleichzeitig kritische Gesundheitsinformationen vor Bedrohungen.



Zuverlässige Speicherlösungen für Überwachungsdaten mit Open-E JovianDSS!

Zukunftssichere CCTV-Infrastruktur
Überwachungs- und Sicherheitsdaten sind wichtiger denn je. Mit Open-E JovianDSS lassen sich steigende Speicheranforderungen sicher bewältigen – unterstützt durch eine Speicherlösung, die hochauflösendes Videomaterial und kontinuierliche Aufzeichnungen effizient verarbeitet. Unser umfassender Leitfaden zeigt optimale Strategien für eine sichere und skalierbare CCTV-Speicherung.

Optimale Strategien für die Datenspeicherung
Ob lokal, in der Cloud oder als Hybridlösung – unsere Broschüre listet die besten Ansätze für individuelle Überwachungsanforderungen. Da Videoqualität und Dateigrößen stetig zunehmen, sorgt Open-E JovianDSS dafür, dass Ihre Technik Schritt hält.

- **Zuverlässiges und effizientes Speichermanagement**
  Jedes einzelne Bildmaterial wird ohne Unterbrechung gesichert. Open-E JovianDSS optimiert die Speicherkapazität, damit Ihre Daten zugänglich und geschützt bleiben.
- **Nahtlose Skalierbarkeit für wachsende Anforderungen**
  Passen Sie Ihre Speicherinfrastruktur mühelos an, wenn die Anforderungen steigen – ganz ohne Herstellerbindung.
- **Sofortige Datenwiederherstellung mit Snapshot-Technologie**
  Verluste und Ausfallzeiten minimieren: Videodatenarchive lassen sich mit Point-in-Time-Snapshots schnell auf den ursprünglichen Stand zurücksetzen.
- **Hybride Lösungen für höhere Sicherheit**
  Kombinieren Sie die Vorteile von lokaler und Cloud-Speicherung für eine umfassende Schutzstrategie. Open-E JovianDSS ermöglicht die perfekte Balance zwischen Zugriff und Sicherheit.

open-e JovianDSS

Stärken Sie Ihr Überwachungssystem mit Expertenwissen.
Scannen Sie den QR-Code oder besuchen
Sie open-e.com für Ihren **kostenlosen Download!**

Beispiele für Behörden und öffentliche Organisationen

mit Open-E-Systemimplementierungen

Mit zahlreichen Implementierungen in Behörden und öffentlichen Institutionen hat sich Open-E JovianDSS als zuverlässige Lösung für sicheres und effizientes Datenmanagement bewährt – und erfüllt selbst strengste gesetzliche Vorgaben. Die Lösung ist flexibel konzipiert und unterstützt sowohl Hardware- als auch Hypervisor-Unabhängigkeit, sodass Institutionen ihre IT-Infrastruktur optimieren und gleichzeitig Betriebskosten senken können – ein entscheidender Faktor für budgetbewusste öffentliche Einrichtungen.

Die Software bietet leistungsstarke Funktionen für Datenschutz, Skalierbarkeit und nahtloses Management. Damit können Behörden und öffentliche Einrichtungen ihre Geschäftskontinuität sicherstellen und ihre Speicherinfrastruktur flexibel an wachsende Anforderungen anpassen. Durch die Unterstützung von Compliance-Standards und die einfache Integration werden IT-Abläufe optimiert, was sichere, leistungsstarke Speicherlösungen in unterschiedlichsten Bereichen des öffentlichen Sektors ermöglicht, zum Beispiel:

- **Ministerien / Behörden**
- **Komunal- / Stadtverwaltungen**
- **Justizeinrichtungen**
- **Strafverfolgungsbehörden**
- **Militäreinheiten**
- **Bildungseinrichtungen**
- **Historische und kulturelle Organisationen**
- **Forschungs- und Wissenschaftsinstitutionen**
- **Öffentliche Versorgungs- und Dienstleistungsunternehmen**
- **Verbraucherschutzbehörden**

open-e

Gegründet 1998 ist Open-E ein etablierter Entwickler von IP-basierter Speicherverwaltungssoftware. Das Flaggschiffprodukt, **Open-E JovianDSS**, ist eine robuste, preisgekrönte Speicheranwendung, die hervorragende Kompatibilität mit Industriestandards bietet. Es ist zudem besonders einfach zu bedienen und zu verwalten. Darüber hinaus zählt es zu den stabilsten Lösungen auf dem Markt und ist unangefochtener Preis-Leistungs-Sieger.

Dank seines hervorragenden Rufs, seiner langjährigen Erfahrung und hohen Verlässlichkeit ist Open-E zum bevorzugten Technologiepartner führender IT-Unternehmen geworden. Weltweit gibt es inzwischen **über 40.000 Installationen.**

+40,000 Software-Implementierungen

+120 Länder weltweit

+25 Jahre Erfahrung

+800 Zertifizierte Ingenieure und Vertriebsprofis

Open-E, Inc. | +1 (678) 666 2880 (US) | +49 (89) 800 777 0 (Europe) | info@open-e.com