open-e

Open-E JovianDSS

DAS DATENSPEICHERSYSTEM FÜR NIS2-KONFORMITÄT UND IHRE UNTERNEHMENSSICHERHEIT



Open-E JovianDSS - Ein Baustein für Ihre NIS2-Konformität

1. Warum NIS2 wichtig ist 4
2. Betroffene Unternehmen & Branchen 5
3. Anforderungen der NIS2-Richtlinie 6
4. Herausforderungen für IT-Prozesse 7
5. Open-E JovianDSS als Lösung für NIS2-Anforderungen 8
6. Weil Sicherheit zählt: Open-E JovianDSS für Ihre NIS2-Strategie 9
7. Rolle von Lieferanten in der Lieferkette 10
8. Angriffspunkte bei Ransomware – Allgemeine Bedrohungen 11
9. Mit Open-E JovianDSS Ransomware-Folgen minimieren 12
10. 10-Punkte-Plan zur Umsetzung der NIS2-Richtlinie 13
11. Weiterführende Informationen und Unterstützung 14



Mehr Cybersicherheit für Unternehmen – Open-E begleitet Sie dabei



Sehr geehrte Partner und Kunden,
Die Einführung der NIS2-Richtlinie markiert einen entscheidenden Schritt hin zu mehr Cybersicherheit und Resilienz in Unternehmen. Für viele stellt die Umsetzung der Anforderungen jedoch eine große Herausforderung dar – von der Sicherstellung der Datenintegrität bis zur Etablierung von Melde- und Wiederherstellungsprozessen.

Mit Open-E JovianDSS möchten wir Ihnen einen wichtigen Baustein für Ihre IT-Strategie bieten, der es Ihnen ermöglicht, die NIS2-Vorgaben effizient umzusetzen. Unsere Lösung unterstützt Sie dabei, Datenverluste zu vermeiden, Ausfallzeiten zu minimieren und Ihre IT-Infrastruktur zukunftssicher zu gestalten.

Ich lade Sie ein, sich in dieser Broschüre über die zentralen Anforderungen der NIS2-Richtlinie und die Vorteile von Open-E JovianDSS zu informieren.

Vielen Dank für Ihr Interesse – wir freuen uns darauf, Sie bei der Erreichung Ihrer IT- und Sicherheitsziele zu begleiten.

Mit freundlichen Grüßen

Krzysztof Franek
CEO, Open-E

Warum NIS2 wichtig ist

Die NIS2-Richtlinie stärkt die digitale Sicherheit in Europa und fordert Unternehmen auf, ihre IT-Systeme widerstandsfähiger zu machen.

Was regelt die NIS2-Richtlinie?

Die NIS2-Richtlinie setzt Standards für den Schutz kritischer Infrastrukturen wie Energie, Gesundheit, Transport und Finanzwesen. Unternehmen müssen Sicherheitsrisiken minimieren, Vorfälle melden und Vorgaben einhalten. Nichtbeachtung führt zu Sanktionen.

- Einheitliche Standards für Netzwerksicherheit in der EU.
- Verpflichtung zur Risikominderung und Vorfallsmeldung.
- Fokus auf kritische Sektoren und wichtige Einrichtungen.
- Sanktionen bei Nichteinhaltung der Vorgaben.

Warum ist NIS2 für Unternehmen wichtig?

Die Richtlinie fordert Unternehmen auf, IT-Prozesse anzupassen und ihre Verantwortung für Sicherheit zu übernehmen. Dies betrifft nicht nur direkte Anforderungen, sondern auch Abhängigkeiten in Lieferketten.

- Stärkere Verpflichtungen zur Risikominderung und Geschäftskontinuität.
- Erweiterte Meldepflichten für Sicherheitsvorfälle.
- Geltung auch für kleinere Unternehmen durch Lieferkettenabhängigkeiten.
- Klare Verantwortlichkeiten für Geschäftsführer bei IT-Sicherheitsvorgaben.

Ab wann gilt dies für deutsche Unternehmen?

- Unternehmen, die unter die NIS2-Richtlinie fallen, müssen sich spätestens ab dem Inkrafttreten des deutschen Umsetzungsgesetzes (voraussichtlich März 2025) an die Vorgaben halten. Ab diesem Zeitpunkt kann es auch Strafen geben.
- Für betroffene Unternehmen empfiehlt es sich jedoch, bereits jetzt Maßnahmen einzuleiten, um die Anforderungen fristgerecht zu erfüllen.

Deutschland

Oktober 2024

Bis dahin müssen EU-Mitgliedstaaten NIS2 in nat. Recht umsetzen.

März 2025 geplant

NIS2UmsuSC

Betroffene Unternehmen & Branchen

Unternehmen, die für die Gesellschaft und Wirtschaft von wesentlicher Bedeutung sind, fallen unter die NIS2-Richtlinie. Dazu gehören kritische Sektoren wie Energie, Gesundheit, Transport und digitale Infrastruktur.

Kriterien für NIS2-Pflicht:

- Tätig in wesentlichen oder wichtigen Sektoren (z. B. Energie, Gesundheit, Transport).
- **Unternehmensgröße:**
  Über 50 Mitarbeiter oder Jahresumsatz über 10 Millionen Euro.
- Unabhängig von Größe, wenn die Branche als kritisch eingestuft wird.

Branchen und Einrichtungen unter NIS2

Wesentliche Einrichtungen:

- Energie (z. B. Strom, Gas, Wasser).
- Gesundheit (z. B. Krankenhäuser, Labore).
- Finanzwesen (z. B. Banken).
- Transport (z. B. Bahn, Luftverkehr).

Wichtige Einrichtungen:

- Digitale Infrastruktur (z. B. Rechenzentren).
- Chemische Industrie.
- Lebensmittelversorgung.

Indirekte Betroffenheit durch Lieferketten

Auch nicht direkt betroffene Unternehmen können über Lieferketten indirekt in den Anwendungsbereich der NIS2 fallen.

Beispiele:

- IT-Dienstleister für kritische Branchen.
- Hersteller und Zulieferer für wesentliche Einrichtungen.
- Logistikunternehmen in kritischen Sektoren.

Empfehlung:

- Sicherheitsmaßnahmen implementieren, um Anforderungen der Kunden zu erfüllen.
- Klare Kommunikation mit Auftraggebern über Sicherheitsvorgaben.
- Moderne Cybersicherheitslösungen einsetzen, wie z. B. Open-E JovianDSS.

Anforderungen der NIS2-Richtlinie

Sicherheitsvorkehrungen und Risikominderung

Die NIS2-Richtlinie fordert Unternehmen dazu auf, robuste Sicherheitsmaßnahmen zu implementieren, um Bedrohungen vorzubeugen und Risiken zu minimieren.

- Implementierung von Firewalls, Intrusion-Detection-Systemen (IDS) und anderen Schutzmechanismen.
- Regelmäßige Schwachstellenanalysen und Penetrationstests.
- Mitarbeiterschulungen zur Sensibilisierung für Cybersicherheitsbedrohungen.
- **Nutzung sicherer Backup- und Wiederherstellungsstrategien, um Datenverluste zu vermeiden.**

Incident-Management und Meldepflichten

Unternehmen müssen in der Lage sein, Sicherheitsvorfälle schnell zu erkennen, zu melden und darauf zu reagieren.

- Einführung eines Incident-Management-Systems zur Erkennung und Analyse von Sicherheitsvorfällen.
- Etablierung von klaren Meldewegen und Reaktionszeiten (meist innerhalb von 24 bis 72 Stunden).
- Dokumentation und Analyse von Vorfällen zur Vermeidung zukünftiger Risiken.
- Zusammenarbeit mit Behörden, um Vorfälle effizient zu melden.

Einhaltung von Branchenspezifischen Standards

Die NIS2-Richtlinie fordert Unternehmen dazu auf, branchenspezifische Sicherheitsstandards einzuhalten, um die Anforderungen effektiv umzusetzen.

- Orientierung an etablierten Standards wie ISO/IEC 27001 oder branchenspezifischen Normen.
- Zusammenarbeit mit Fachverbänden, um Best Practices zu übernehmen.
- Überprüfung der eigenen Prozesse auf Konformität mit regulatorischen Vorgaben.
- Nutzung von Tools und Technologien, die den jeweiligen branchenspezifischen Anforderungen gerecht werden.

Business Continuity und Disaster Recovery

Die Sicherstellung der Betriebsfähigkeit im Falle eines Vorfalls ist ein zentraler Bestandteil der NIS2-Richtlinie.

- Erstellung eines Business-Continuity-Plans (BCP), der auch Cyberbedrohungen berücksichtigt.
- Regelmäßige Tests von Notfallplänen, um die Effektivität zu gewährleisten.
- **Nutzung von Technologien wie Hochverfügbarkeits-Clustern und redundanter Infrastruktur.**
- **Einrichtung von On- und Off-Site-Backups für schnelle Datenwiederherstellung.**

Diese vier Bereiche bilden das Fundament für die Umsetzung der NIS2-Richtlinie und erfordern eine ganzheitliche Betrachtung der IT- und Sicherheitsstrategie eines Unternehmens. Open-E JovianDSS kann dabei als Baustein dienen, insbesondere bei der Sicherstellung von Business Continuity und einer effektiven Backup-Strategie.

Herausforderungen für IT-Prozesse

Die Umsetzung der NIS2-Richtlinie erfordert umfassende Anpassungen in den IT-Prozessen, von der Infrastruktur bis hin zur Datensicherung. Open-E JovianDSS bietet dabei zuverlässige Lösungen für Geschäftskontinuität und Datensicherheit.

Anpassungsbedarf im IT-Bereich

- § Integration moderner Technologien zur Erfüllung neuer Sicherheitsstandards.
- § Überarbeitung von Prozessen für Meldepflichten und Sicherheitsanforderungen.
- § Schulung von Mitarbeitern zur Umsetzung der Richtlinie.

Open-E JovianDSS unterstützt durch flexible Integration und Hochverfügbarkeitslösungen.

Risikoanalysen und Sicherheitsüberprüfungen

- § Identifikation von Schwachstellen und kritischen IT-Systemen.
- § Sicherstellung der Datenintegrität und Recovery-Fähigkeit.

Funktionen wie Snapshots und Selbstheilung von Open-E JovianDSS minimieren Risiken.

Entwicklung einer sicheren Backup- und Wiederherstellungsstrategie

- § Daten sowohl On-Site als auch Off-Site sichern.
- § Schnelle Wiederherstellung bei Ausfällen gewährleisten.
- § Einsatz von Hochverfügbarkeitslösungen
- § zur Minimierung von Ausfallzeiten.

Mit asynchroner Replikation und Snapshots bietet Open-E JovianDSS eine starke Basis.

Fazit:

Die Herausforderungen der NIS2-Richtlinie im Bereich der IT-Prozesse sind umfangreich, aber lösbar. Mit der Unterstützung von Open-E JovianDSS können Unternehmen nicht nur die Anforderungen erfüllen, sondern auch ihre IT-Infrastruktur zukunftssicher gestalten.

Open-E JovianDSS als Lösung für NIS2-Anforderungen

Die NIS2-Richtlinie verlangt von Unternehmen robuste Maßnahmen zur Sicherstellung der Datensicherheit und Geschäftskontinuität. Open-E JovianDSS bietet eine leistungsstarke und flexible Lösung, die Unternehmen bei der Erfüllung dieser Anforderungen unterstützt.

Unterstützung bei der Einhaltung der NIS2-Richtlinie

Mit Open-E JovianDSS erhalten Unternehmen einen wichtigen Baustein, um die komplexen Vorgaben der NIS2-Richtlinie umzusetzen und die Verfügbarkeit sowie Integrität ihrer Daten zu sichern.

Schlüsselmerkmale: Hochverfügbarkeit, Snapshots und Datenreplikation

Open-E JovianDSS bietet unverzichtbare Technologien, um Daten jederzeit verfügbar zu halten und schnell auf Vorfälle reagieren zu können.

Förderung von Geschäftskontinuität und Datensicherheit

Durch robuste Sicherheitsmechanismen und modernste Backup-Strategien ermöglicht Open-E JovianDSS selbst in Krisensituationen einen reibungslosen Geschäftsbetrieb.

Fazit:
Open-E JovianDSS ist ein unverzichtbarer Baustein für Unternehmen, die die Anforderungen der NIS2-Richtlinie erfüllen und gleichzeitig höchste Standards in Datensicherheit und Geschäftskontinuität setzen möchten.

Weil Sicherheit zählt: Open-E JovianDSS für Ihre NIS2-Strategie

open-e JovianDSS

Die NIS2-Richtlinie fordert neue IT-Sicherheitsstandards. Open-E JovianDSS schützt Ihre Daten, minimiert Ausfallzeiten und unterstützt Sie bei der Umsetzung. Sichern Sie Ihre IT zukunftssicher!

- Hochverfügbarkeit (Active-Active/Active-Passive Cluster)
- Unbegrenzte Snapshots und Klone
- Asynchrone Replikation für Off-Site-Sicherheit
- Inline-Komprimierung und Deduplizierung für optimale Speichernutzung
- Hardware-unabhängige, skalierbare Softwarelösung
- Unterstützung für branchenspezifische Standards
- Intuitiv über Web-GUI und REST API

Mit Open-E JovianDSS: Sicherheit und Effizienz für NIS2.

Jetzt Beratung sichern!



Rolle von Lieferanten in der Lieferkette

Indirekte Auswirkungen der NIS2-Richtlinie

- Auch Unternehmen, die selbst nicht direkt unter die NIS2-Richtlinie fallen, können betroffen sein. Als Teil der Lieferkette müssen sie ebenfalls hohe Sicherheitsstandards einhalten, um die Anforderungen ihrer Auftraggeber zu erfüllen.

Bedeutung von Cybersicherheitslösungen

- Für Zulieferer wird der Einsatz moderner Cybersicherheitslösungen essenziell, um Datenintegrität und Geschäftskontinuität sicherzustellen und Vertrauen in der Lieferkette zu stärken.

Sind Sie als Liefernant von NIS2 betroffen?

Stärken Sie Ihren IT Prozess mit Open-E JovianDSS.

Nehmen Sie Kontakt mit uns auf:

Angriffspunkte bei Ransomware – Allgemeine Bedrohungen

Ransomware-Angriffe nutzen Schwachstellen in IT-Infrastrukturen aus, um Unternehmen zu schädigen.
Einige Schwachstellen erfordern allgemeine Sicherheitsmaßnahmen, da sich Bedrohungen in unzureichend gesicherten Netzwerken ungehindert ausbreiten können.

Angriffspunkte ohne Open-E JovianDSS-spezifischen Schutz:

- **Manipulation durch Phishing und Social Engineering:**
  Mitarbeiter werden durch täuschende E-Mails dazu verleitet, schädliche Anhänge zu öffnen.
  Lösung: Schulungen, Anti-Phishing-Software und E-Mail-Filter.

- **Missbrauch privilegierter Zugänge:**
  Schwache Passwörter oder fehlende Multi-Faktor-Authentifizierung eröffnen Angreifern Zugriff auf kritische Bereiche.
  Lösung: Einführung von MFA und striktem Benutzerrechte-Management.

- **Veraltete Software und Systeme:**
  Ungepatchte Schwachstellen bieten Hackern einfache Angriffsflächen.
  Lösung: Regelmäßige Updates und ein automatisiertes Patch-Management-System.

Mit Open-E JovianDSS Ransomware-Folgen minimieren

Open-E JovianDSS schützt nicht vor den Angriffen selbst, sondern minimiert die Auswirkungen durch unveränderliche Backups, Hochverfügbarkeit und asynchrone Replikation. Diese Funktionen ermöglichen es, verschlüsselte oder verlorene Daten schnell wiederherzustellen und die Geschäftskontinuität aufrechtzuerhalten.

→ Immutable Snapshots:

Ransomware kann Daten nicht verändern oder löschen – Snapshots bleiben unverändert erhalten.

→ Asynchrone Replikation:

Backups an externen Standorten bieten zusätzliche Sicherheit und Unabhängigkeit vom Produktionssystem.

→ Hochverfügbarkeit:

Redundante Hardware sichert den Geschäftsbetrieb während der Wiederherstellung betroffener Systeme.

→ Automatisierte Wiederherstellung:

Snapshots und Klone ermöglichen die schnelle Wiederherstellung von intakten Daten.

Mit Open-E JovianDSS erhalten Sie einen zuverlässigen Schutz vor Datenverlust und Ausfällen. Kombiniert mit allgemeinen Sicherheitsmaßnahmen wie Mitarbeiterschulungen und Patch-Management können Sie eine umfassende IT-Sicherheitsstrategie umsetzen.

10-Punkte-Plan zur Umsetzung der NIS2-Richtlinie

1. **Bestandsaufnahme durchführen**
   Kritische IT-Systeme identifizieren und Sicherheitsstatus bewerten.
2. **Risikobewertung erstellen**
   Potenzielle Bedrohungen analysieren und Maßnahmen priorisieren.
3. **Schutzmaßnahmen priorisieren**
   Sicherheitslücken schließen und Schwachstellen beheben.
4. **Backup-Strategie entwickeln**
   Kombination aus On-Site- und Off-Site-Backups planen.
5. **Disaster-Recovery-Pläne umsetzen**
   Notfallpläne für schnelle Betriebswiederaufnahme erstellen.
6. **Automatisierte Prozesse einrichten**
   Snapshots und Replikation für kontinuierliche Datensicherung nutzen.
7. **Monitoring und Alarmierung implementieren**
   Echtzeit-Monitoring-Tools zur Bedrohungserkennung einsetzen.
8. **Meldeprozesse definieren**
   Sicherheitsvorfälle fristgerecht an Behörden melden.
9. **Notfalltests durchführen**
   Regelmäßige Tests von Backup-, Recovery- und Krisenmanagement-Plänen.
10. **Mitarbeiter schulen und sensibilisieren**
    IT-Teams und Mitarbeiter auf Sicherheitsanforderungen vorbereiten.

Open-E JovianDSS als starker Baustein

Mit Open-E JovianDSS setzen Sie viele dieser Schritte effizient um:

- **Snapshots und Replikation** sichern Daten und ermöglichen schnelle Wiederherstellung.
- **Hochverfügbarkeitslösungen** minimieren Ausfallzeiten.
- **Echtzeit-Monitoring** sorgt für frühzeitige Bedrohungserkennung.

So schaffen Sie die Grundlage für Datensicherheit, Geschäftskontinuität und eine starke IT-Infrastruktur.

Weiterführende Informationen und Unterstützung

Open-E JovianDSS:

Open-E JovianDSS bietet essenzielle Funktionen, um die Anforderungen der NIS2-Richtlinie umzusetzen:

- → **Hochverfügbarkeitslösungen:** Minimieren Sie Ausfallzeiten durch Active-Active-Cluster.
- → **Datenreplikation:** Sichern Sie Daten On- und Off-Site mit asynchroner Replikation.
- → **Automatisierte Snapshots:** Schützen Sie Daten kontinuierlich und stellen Sie sie schnell wieder her.
- → **Selbstheilungsmechanismen:** Verhindern Sie Datenkorruption durch automatische Fehlerkorrektur.
- → **Effiziente Speicherverwaltung:** Optimieren Sie Ressourcen mit Inline-Komprimierung und Deduplizierung.

Entdecken Sie, wie Open-E JovianDSS Ihre IT-Infrastruktur stärkt und Ihre Datensicherheit gewährleistet.

Open-E Academy:

In der Open-E Academy finden Sie umfassende Schulungsangebote, um das Potenzial von Open-E JovianDSS voll auszuschöpfen.

- → **Technische Handbücher:** Schritt-für-Schritt-Anleitungen für alle Funktionen.
- → **Video-Tutorials:** Praktische Erklärungen für den effektiven Einsatz.
- → **OECE Trainings:** Zertifizierte Programme, um IT-Teams und Partner im Umgang mit Open-E JovianDSS zu schulen und seine Funktionen optimal zu nutzen.
- → Lernen Sie, wie Sie mit Open-E JovianDSS Datensicherheit und Geschäftskontinuität effizient umsetzen.

Open-E JovianDSS: Flexibel und Hypervisor-unabhängig

open-e JovianDSS

Sichern Sie Ihre Daten unabhängig von Ihrer Virtualisierungsplattform!

Mit Open-E JovianDSS profitieren Sie von einer hypervisor-unabhängigen Speicherlösung, die maximale Flexibilität und nahtlose Integration in Ihre IT-Infrastruktur ermöglicht.

Hauptvorteile:

- ✓ Hypervisor-unabhängig: Unterstützt VMware, Hyper-V, Proxmox VE und viele weitere Plattformen
- ✓ Hochverfügbarkeit und Business Continuity: Verhindern Sie Ausfallzeiten und sichern Sie Ihre Daten zuverlässig
- ✓ Skalierbarkeit und Effizienz: Optimieren Sie Ihre Speicherressourcen und passen Sie sich flexibel an wachsende Anforderungen an



Kostenlose Broschüre herunterladen und mehr erfahren:

open-e

Gegründet im Jahr 1998, ist Open-E ein etablierter Entwickler von IP-basierter Storage-Management-Software. Das Flaggschiff-Produkt, Open-E JovianDSS, ist eine robuste, preisgekrönte Speicheranwendung, die hervorragende Kompatibilität mit Branchenstandards bietet. Es ist zudem besonders benutzerfreundlich und einfach zu verwalten. Darüber hinaus zählt es zu den stabilsten Lösungen auf dem Markt und ist ein unangefochtener Preis-Leistungs-Sieger.

Dank seines hervorragenden Rufs, seiner Erfahrung und seiner Zuverlässigkeit ist Open-E zum bevorzugten Technologiepartner führender IT-Unternehmen geworden. Open-E kann weltweit über 40.000 Installationen vorweisen.

+40,000 Software Implementierungen

+120 Länder weltweit

+25 Jahre Erfahrung

+800 zertifizierte Ingenieure und Vertriebsprofis

ABC SYSTEMS AG

APPLIED BRAINWARE & COMPUTER SYSTEMS

Schlieren, Bern, Zug +41 43 433 6 433 www.abcsystems.ch

Open-E GmbH | +49 (89) 800 777 0 (Europe) | info@open-e.com