Next-Gen Defense

mit Open-E JovianDSS Effektiver Schutz vor den Folgen von Ransomware-Angriffen

Inhaltsverzeichnis

Einleitung

Ransomware ist eine Schadsoftware, die den Zugriff auf Computersysteme oder Daten blockiert – bis ein Lösegeld gezahlt wird.

Oft verschlüsselt diese Malware Dateien, macht sie für die Nutzer unzugänglich und fordert anschließend eine Zahlung für den Schlüssel zur Entschlüsselung. Ransomware-Angriffe können verheerend sein: Sie führen zu erheblichem Datenverlust, finanziellen Schäden und einem Reputationsverlust.

In den letzten Jahren ist die Zahl der Ransomware-Vorfälle stark gestiegen – betroffen sind Unternehmen, Gesundheitseinrichtungen und Behörden. Solche Angriffe können den Betrieb lahmlegen, hohe Wiederherstellungskosten verursachen und das Vertrauen von Kunden nachhaltig schädigen.

Umso wichtiger ist es, Ransomware zu verstehen und starke Schutzmaßnahmen zu implementieren – sie sind entscheidend für die Cybersicherheit jeder Organisation.

Zentrale Cybersecurity-Bedrohungen im Jahr 2025 und darüber hinaus

Open-E analysiert: Neue Bedrohungen im Bereich Cybersicherheit

Zu den aktuellen Entwicklungen zählen KI-gesteuerte Malware, Deepfake-Betrugsmaschen und die verstärkte Angriffsfläche durch IoT-Geräte. Um sich proaktiv schützen zu können, ist ein gutes Verständnis dieser Bedrohungen unerlässlich.

- **KI-gesteuerte Malware**

  Diese Art von Schadsoftware stellt eine hochentwickelte Weiterentwicklung dar: Sie nutzt künstliche Intelligenz, um ihre Fähigkeiten dynamisch anzupassen. Solche Angriffe können sich in Echtzeit an Sicherheitsmaßnahmen anpassen – und sind dadurch schwerer zu erkennen und zu neutralisieren. KI-basierte Malware kann komplexe Aufgaben übernehmen, z. B. das Umgehen von Erkennungssystemen, das automatisierte Ausnutzen von Schwachstellen sowie das Lernen aus dem Verhalten der Verteidigungssysteme, um ihre Angriffsstrategien ständig zu optimieren.

- **Deep Fake-Betrug**

  Deep Fake-Technologien nutzen KI, um täuschend echte Bilder, Stimmen und Videos zu erzeugen – mit erheblichen Risiken für Einzelpersonen und Unternehmen. Sie können für Identitätsdiebstahl, Finanzbetrug oder die gezielte Verbreitung von Falschinformationen missbraucht werden. Durch die überzeugende Imitation realer Personen stellen Deep Fakes ein wirkungsvolles Werkzeug für Social-Engineering-Angriffe dar und können sensible Informationen gefährden oder dem Ruf eines Unternehmens schaden.

- **Gezielte Angriffe auf IoT-Geräte**

  Die zunehmende Verbreitung vernetzter Geräte – vom Smart Home bis zur industriellen Steuerung – schafft eine große und oft unzureichend geschützte Angriffsfläche. Cyberkriminelle nutzen Schwachstellen in IoT-Geräten aus, da diese häufig nur über begrenzte Sicherheitsmaßnahmen verfügen. Betroffene Geräte können zur Durchführung groß angelegter Angriffe wie DDoS-Attacken verwendet werden oder als Einstiegspunkt für den Zugriff auf sensible Netzwerke und Daten dienen.

Die Zukunft der Cybersicherheit: Entwicklungen und Herausforderungen

Die Bedrohungslage in der IT-Sicherheit entwickelt sich stetig weiter – mit zunehmend ausgeklügelten Angriffsmethoden. Deshalb müssen Organisationen agile und adaptive Sicherheitsstrategien verfolgen, um Angreifern immer einen Schritt voraus zu sein.

Advanced Persistent Threats (APTs)

APTs sind langfristig angelegte, gezielte Cyberangriffe, die meist von hochqualifizierten und gut finanzierten Angreifern durchgeführt werden. Ziel ist es, sensible Daten zu stehlen oder Geschäftsprozesse unbemerkt zu stören. Unternehmen müssen ihre Sicherheitsmaßnahmen kontinuierlich überwachen und anpassen, um solche schwer erkennbaren Eindringversuche frühzeitig zu entdecken und wirksam zu bekämpfen.

KI und Machine Learning in der Cybersicherheit

Künstliche Intelligenz und maschinelles Lernen unterstützen die IT-Sicherheit durch automatisierte Bedrohungserkennung und Reaktionsmechanismen. Sie analysieren große Datenmengen, um Muster und Anomalien zu erkennen, die auf Angriffe hinweisen. Diese proaktive Herangehensweise ermöglicht es Unternehmen, komplexe Angriffe frühzeitig zu erkennen und gezielt zu entschärfen.

Regulatorische Änderungen und Compliance

Mit neuen Datenschutzgesetzen und branchenspezifischen Vorschriften müssen Unternehmen ihre Sicherheitsrichtlinien regelmäßig anpassen, um gesetzeskonform zu bleiben und Bußgelder zu vermeiden. Wer auf dem Laufenden bleibt, schützt nicht nur seine Daten, sondern erhält auch das Vertrauen seiner Kunden – besonders in einem zunehmend regulierten Umfeld.

Zero-Trust-Architektur

Die Zero-Trust-Architektur basiert auf dem Prinzip, dass kein Benutzer oder Gerät – egal ob innerhalb oder außerhalb des Netzwerks – automatisch als vertrauenswürdig gilt. Jeder Zugriff auf Ressourcen muss kontinuierlich verifiziert werden. Dieses Sicherheitsmodell reduziert das Risiko von Datenpannen durch strikte Zugriffskontrollen und die lückenlose Überwachung aller Netzwerkaktivitäten.

Einen Schritt voraus: Schutz durch vorausschauende Maßnahmen

Vorausschauende Sicherheitsstrategien – wie regelmäßige Sicherheitsbewertungen und der Einsatz modernster Technologien – sind essentiell, um eine starke Cybersicherheitsstruktur aufrechtzuerhalten.

- **Regelmäßige Sicherheitsbewertungen**

  Durch systematische Sicherheitsanalysen werden Schwachstellen und Risiken in der IT-Infrastruktur frühzeitig erkannt – bevor Angreifer sie ausnutzen können. So wird sichergestellt, dass bestehende Schutzmaßnahmen aktuell und wirksam sind und potenzielle Bedrohungen gezielt adressiert werden.

- **Einsatz modernster Technologien**

  Der Einsatz neuester Sicherheitstechnologien – etwa Verschlüsselung, Blockchain oder Firewalls der nächsten Generation – stärkt den Schutz gegenüber neuen Angriffsszenarien. Diese Innovationen sorgen dafür, dass Sicherheitsarchitekturen flexibel bleiben und sich gegen hochentwickelte Cyberangriffe behaupten können.

- **Kontinuierliche Überwachung und Bedrohungsanalyse**

  Durch permanente Netzwerküberwachung lassen sich Bedrohungen in Echtzeit erkennen und schnell darauf reagieren. Die Integration von Threat Intelligence hilft dabei, neue Angriffsmethoden frühzeitig zu identifizieren und entsprechende Gegenmaßnahmen proaktiv zu ergreifen.

- **Schulung und Sensibilisierung der Mitarbeitenden**

  Gezielte Schulungsprogramme und Awareness-Kampagnen machen Mitarbeitende mit aktuellen Bedrohungen und Sicherheitspraktiken vertraut. Eine gut informierte Belegschaft ist entscheidend für die IT-Sicherheit, denn menschliches Fehlverhalten zählt zu den häufigsten Ursachen für Sicherheitsvorfälle.

- **Entwicklung und Test von Notfallplänen**

  Durch das Erstellen und regelmäßige Testen von Incident-Response-Plänen stellen Unternehmen sicher, dass sie im Ernstfall schnell und effektiv reagieren können. Solche Pläne helfen, Sicherheitsvorfälle zu bewältigen, Ausfallzeiten zu minimieren und Datenverluste zu vermeiden.

SCHÜTZEN SIE IHR UNTERNEHMEN VOR DEN FOLGEN VON RANSOMWARE-ANGRIFFEN MIT OPEN-E JOVIANDSS!

BEFREIEN SIE SICH 2025 VOM VENDOR-LOCK-IN!

Willkommen in der Zukunft der Datensicherheit – 2025 steht ganz im Zeichen hypervisorunabhängiger Speicherlösungen. Wählen Sie Ihre Hardware, setzen Sie den Hypervisor Ihrer Wahl ein und kombinieren Sie beides mit Open-E JovianDSS – für vollständige Freiheit ohne Herstellerbindung. Skalieren Sie Ihre Speicherlösung, optimieren Sie die Leistung und schützen Sie Ihre Daten, ohne Ihre laufenden Geschäftsprozesse zu unterbrechen. Warten Sie nicht, bis ein Ransomware-Angriff zuschlägt. Schützen Sie Ihre Daten und stellen Sie Ihre Geschäftskontinuität sicher – mit Open-E JovianDSS. Kontaktieren Sie uns noch heute, um mehr zu erfahren oder eine Demo zu vereinbaren. Gemeinsam sichern wir Ihre Datenzukunft. Handeln Sie jetzt.

Fortschrittliche Snapshot-Technologie

Stoppen Sie Ransomware im entscheidenden Moment: Open-E JovianDSS erstellt sofortige Snapshots Ihrer Daten – sicher, isoliert und unveränderbar. Im Ernstfall einfach auf einen sauberen Wiederherstellungspunkt zurückspringen – schnell und zuverlässig.

Intelligente Aufbewahrungsrichtlinien

Verabschieden Sie sich von unnötigem Speicherverbrauch! Passen Sie Ihre Aufbewahrungspläne individuell an – schützen Sie kritische Daten genau so lange, wie nötig, und schaffen Sie gleichzeitig wertvollen Speicherplatz.

SED-Verschlüsselung für maximale Sicherheit

Sichern Sie Ihre Daten mit selbstverschlüsselnden Laufwerken (SEDs)! Open-E JovianDSS arbeitet nahtlos mit Hardware-Verschlüsselung – so bleiben Ihre Daten selbst bei einem Angriff geschützt. Ist die Verschlüsselung aktiv, haben Hacker keine Chance.

Geschäftskontinuität & Desaster Recovery

Ihr Unternehmen muss weiterlaufen – auch im Ernstfall! Open-E JovianDSS liefert hochverfügbare Cluster (HA) und zuverlässige On-/Offsite-Backups. So bleibt der Zugriff auf Ihre Daten auch bei Angriffen oder Hardware-Ausfällen jederzeit gesichert – und Sie können schnell wieder durchstarten.

Skalierbarer, hypervisorunabhängiger Speicher

Zukunftssichere Infrastruktur: Wählen Sie den Hypervisor Ihrer Wahl – ohne Vendor Lock-in. Skalieren Sie Ihre Umgebung mit dem Wachstum Ihres Unternehmens und behalten Sie jederzeit die volle Kontrolle.

Ransomware verstehen – Historie und Arten

Ein Blick auf die Geschichte und Typen von Ransomware lohnt sich: Er zeigt, wie groß die Bedrohung bereits war – und wie schnell die Aktivitäten von Cyberkriminellen zunehmen. Im Folgenden sind einige der wichtigsten Entwicklungen dargestellt, die maßgeblich beeinflusst haben, wie Cyberterrorismus heute funktioniert – und welche Richtung er künftig einschlagen könnte.

Historie

1989: Der AIDS-Trojaner (PC Cyborg)

- **Ursprung:** Entwickelt von Joseph Popp gilt der AIDS--Trojaner als erste bekannte Ransomware.
- **Mechanismus:** Die Malware wurde per Diskette an Teilnehmer einer WHO-Konferenz verteilt. Sie verschlüsselte Dateinamen und forderte 189 $ Lösegeld, das an ein Postfach in Panama gesendet werden sollte.
- **Bedeutung:** Diese frühe Form von Ransomware nutzte einfache Verschlüsselung und zeigte erstmals das Potenzial finanzieller Erpressung durch Schadsoftware.

Frühe 2000er: Weiterentwicklung der Ransomwaree

- **Innovation:** Nach dem AIDS-Trojaner kam es zunächst zu einer ruhigeren Phase in der Ransomware-Aktivität. Ab den frühen 2000er-Jahren traten jedoch zunehmend ausgefeiltere Angriffsmethoden auf.
- **Mechanismus:** Erste Varianten wie GPcode nutzten fortschrittlichere Verschlüsselungstechniken, um Dateien zu sperren und Lösegeldforderungen zu stellen.

2005: GPcode

- **Innovation:** GPcode war ein frühes Beispiel für Ransomware mit RSA-Verschlüsselung.
- **Mechanismus:** Die Malware verschlüsselte Dateien auf dem betroffenen Computer und forderte ein Lösegeld für den Schlüssel zur Entschlüsselung. Zwar war die Verschlüsselung technisch noch schwach und konnte teilweise geknackt werden, doch GPcode markierte den Beginn einer zunehmend professionellen Verschlüsselung in der Ransomware-Entwicklung.

2011: WinLock

- **Innovation:** WinLock stellte eine bedeutende Weiterentwicklung der Ransomware-Strategien dar.
- **Mechanismus:** Anders als bisherige Varianten verschlüsselte WinLock keine Dateien, sondern sperrte den gesamten Bildschirm und zeigte ein Bild mit einer Zahlungsaufforderung an. Diese Variante zielte auf Nutzer in Russland ab und forderte Zahlungen über Premium-SMS-Dienste.

2017: WannaCry

- **Innovation:** WannaCry nutzte eine Schwachstelle in Windows-Systemen namens EternalBlue aus, um sich rasch über Netzwerke zu verbreiten.
- **Mechanismus:** Die Verbreitung erfolgte wurmartig: Dateien wurden verschlüsselt und ein Lösegeld in Bitcoin gefordert. WannaCry betraf über 200.000 Computer in 150 Ländern, darunter auch kritische Infrastrukturen wie den britischen Gesundheitsdienst NHS. Der Angriff zeigte eindrucksvoll, wie gefährlich Ransomware in Kombination mit nicht gepatchter Software sein kann.

2022: Conti

- **Innovation:** Conti setzte auf das „Ransomware-as-a-Service"-Modell (RaaS), bei dem Partnergruppen die Angriffe ausführten und dafür an den Lösegeldern beteiligt wurden.
- **Mechanismus:** Die Infektion erfolgte über eine Kombination aus Phishing-E-Mails und Angriffen auf Remote-Desktop-Protokolle (RDP). Nach dem Eindringen wurden Dateien verschlüsselt und Lösegeld gefordert.

2013: Cryptolocker

- **Innovation:** Cryptolocker gilt als Meilenstein in der Ransomware-Geschichte – durch starke Verschlüsselung und große Verbreitung.
- **Mechanismus:** Die Verbreitung erfolgte über Phishing-E-Mails mit schädlichen Anhängen. Nach der Ausführung wurden Dateien auf dem Rechner per RSA-2048 verschlüsselt. Die Täter forderten ein Lösegeld in Bitcoin. Cryptolocker infizierte über 250.000 Systeme und erpresste Millionenbeträge.

2020: Maze

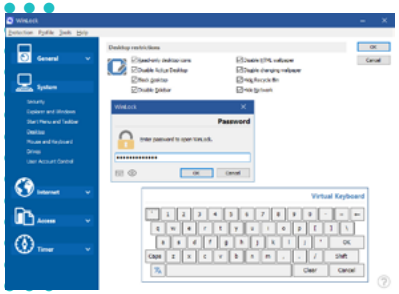
- **Innovation:** Maze machte die Taktik der doppelten Erpressung populär: Neben der Verschlüsselung drohten die Angreifer, sensible Daten zu veröffentlichen, wenn kein Lösegeld gezahlt wurde.
- **Mechanismus:** Die Verbreitung erfolgte über Phishing-E-Mails und Exploit-Kits. Dateien wurden verschlüsselt, gleichzeitig wurden vertrauliche Daten entwendet.

Arten von Ransomware

Crypto-Ransomware

Mechanismus: Verschlüsselt Dateien auf dem System des Opfers und macht sie ohne Entschlüsselungsschlüssel unzugänglich.
Beispiele: Cryptolocker, Locky, WannaCry
Auswirkung: Dies ist eine der häufigsten Ransomware-Formen. Sie zielt meist auf kritische Daten ab und fordert ein Lösegeld für den Zugriff auf die verschlüsselten Dateien.

Quelle: wikipedia.org



Locker-Ransomware

Mechanismus: Sperrt das gesamte System oder Gerät, sodass weder auf Dateien noch auf Anwendungen zugegriffen werden kann.
Beispiel: WinLock
Auswirkung: Im Gegensatz zu Crypto-Ransomware verschlüsselt Locker-Ransomware keine Dateien, sondern blockiert die Benutzeroberfläche. Das Opfer sieht eine Lösegeldforderung zur Freischaltung des Systems.

Quelle: crystaloffice.com

Scareware

Mechanismus: Nutzt gefälschte Warnmeldungen und Bedrohungen, um Opfer zur Zahlung eines Lösegelds zu bewegen. Oft als Antiviren- oder Systemoptimierungssoftware getarnt, die vorgibt, das System sei infiziert.
Beispiele: Gefälschte Antivirenprogramme mit dauerhaften Pop-up-Warnungen
Auswirkung: Diese Form ist meist weniger schädlich, da sie weder Dateien verschlüsselt noch Systeme blockiert. Dennoch kann sie zu erheblicher Verunsicherung und finanziellen Verlusten führen, wenn Zahlungen geleistet werden.

Quelle: signal.avg.com

Doxware (Extortionware)

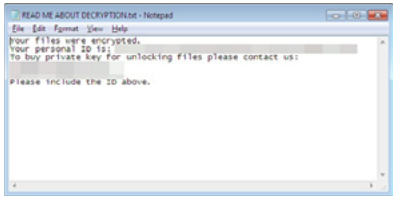
Mechanismus: Droht mit der Veröffentlichung oder dem Leak sensibler Daten, sofern kein Lösegeld gezahlt wird. Verbindet Dateiverschlüsselung mit der Bedrohung durch Datenveröffentlichung.
Beispiel: Maze-Ransomware
Auswirkung: Diese Art nutzt den möglichen Reputationsschaden für das Opfer aus, etwa durch die Veröffentlichung von Kundendaten oder vertraulichen Informationen. Häufig betroffen sind Unternehmen mit sensiblen Kundendaten.

Quelle: media.kasperskycontenthub.com

RaaS (Ransomware as a Service)

Mechanismus: Ein Geschäftsmodell, bei dem Ransomware-Entwickler ihre Tools an Partner verkaufen oder vermieten, die dann die Angriffe ausführen. Die Gewinne werden zwischen den Entwicklern und den Angreifern aufgeteilt.
Beispiele: Sodinokibi (REvil), GandCrab
Auswirkung: Dieses Modell hat Ransomware-Angriffe demokratisiert, da sie auch technisch weniger versierten Kriminellen zugänglich gemacht wurden – was zu einer deutlichen Zunahme der Angriffe führte.

Quelle: pcrisk.pl



Fileless Ransomware

Mechanismus: Läuft vollständig im Arbeitsspeicher des Systems und nutzt legitime Systemtools für den Angriff, ohne klassische Malware-Dateien auf der Festplatte zu hinterlassen.
Beispiel: Sorebrect
Auswirkung: Diese Art ist schwerer zu erkennen und zu entfernen, da sie keine typischen Spuren auf der Festplatte hinterlässt.

Quelle: trendmicro.com

Mobile Ransomware

Mechanismus: Zielt auf mobile Endgeräte ab, sperrt diese oder verschlüsselt gespeicherte Daten.
Beispiele: Koler, Simplocker
Auswirkung: Mobile Ransomware kann besonders störend wirken – gerade vor dem Hintergrund, dass mobile Geräte zunehmend für sensible Transaktionen genutzt werden.

Quelle: webroot.com

KI-gestützte Ransomware

Mechanismus: Nutzt Künstliche Intelligenz zur Erstellung täuschend echter Phishing-E-Mails, Deepfake-Stimmen oder Videos, um Nutzer zur Preisgabe von Zugangsdaten oder zur Ausführung schadhafter Aktionen zu verleiten. Die Malware kann sich dynamisch anpassen, um Sicherheitslösungen zu umgehen..
Beispiele: Deepfake-CEO-Betrug, KI-generierte Spear-Phishing-Mails (noch keine benannten Malware-Familien – aktueller Trend)
Auswirkung: Diese Methode erhöht die Erfolgsquote von Social-Engineering-Angriffen, unterläuft klassische Erkennungssysteme und ermöglicht auch weniger erfahrenen Angreifern personalisierte, skalierbare Angriffe.

Quelle: www.cybersecurityintelligence.com/blog/ransomware-trends-and-top-six-predictions-for-2025-8267.html

Der Ablauf – So funktioniert ein Ransomware-Angriff

Wer versteht, wie Ransomware funktioniert, kann sich besser dagegen schützen. Durch Kenntnis der einzelnen Phasen eines Angriffs können sich Betroffene besser vorbereiten, Angriffe verhindern und im Ernstfall schneller reagieren. Nachfolgend ein Überblick über die typischen Schritte eines Ransomware-Angriffs – von der ersten Infektion bis zur Auswirkung auf das System.

Erster Zugriff

- **Exploit Kits**
  Angreifer nutzen sogenannte Exploit-Kits, um Sicherheitslücken in Betriebssystemen oder Software auszunutzen und sich Zugriff zu verschaffen. Über Remote-Desktop-Protokolle (RDP) können sie Systeme mit schwacher Konfiguration übernehmen und die Ransomware manuell einschleusen.
- **Phishing-E-Mails**
  Die häufigste Methode: Phishing-E-Mails mit schädlichen Anhängen oder Links. Öffnet ein Benutzer den Anhang oder klickt auf den Link, wird die Ransomware auf das System heruntergeladen und ausgeführt.

Verschlüsselung

- **Dateiverschlüsselung**
  Nach der Infektion beginnt die Ransomware mit der Verschlüsselung von Dateien – häufig betroffen sind Dokumente, Datenbanken und andere kritische Inhalte. Die verschlüsselten Dateien werden meist umbenannt (z. B. mit einer neuen Dateiendung), um den Sperrstatus zu kennzeichnen.
- **Systemblockierung**
  Manche Ransomware-Varianten blockieren nicht nur einzelne Dateien, sondern das gesamte System. Es erscheint eine Lösegeldforderung auf dem Bildschirm, der Zugriff auf Dateien oder das Betriebssystem wird vollständig verhindert.

Zustellung der Lösegeldforderung

Lösegeldforderung

Die Ransomware zeigt eine Lösegeldnachricht an – meist als Textdatei oder Bildschirmanzeige. Darin wird dem Opfer erklärt, wie das Lösegeld zu zahlen ist, um die verschlüsselten Dateien wiederherzustellen. Die Nachricht enthält in der Regel Zahlungsanweisungen, oft in Kryptowährung, um die Anonymität des Angreifers zu wahren.

Kommunikationswege

Häufig enthält die Nachricht auch Kontaktmöglichkeiten zum Angreifer – etwa eine E-Mail-Adresse oder einen Link zu einer Darknet--Seite, um über das weitere Vorgehen zu verhandeln oder die Zahlung zu bestätigen. (Beispielquellen: IBM – USA; McAfee)

Zahlung

Entschlüsselungsschlüssel

Nach der Zahlung kann der Angreifer einen Entschlüsselungsschlüssel oder ein Tool bereitstellen, um die verschlüsselten Dateien wieder freizugeben – eine Garantie dafür gibt es jedoch nicht. Die Zahlung erhöht zudem das Risiko, weitere kriminelle Aktivitäten zu fördern.

Lösegeldzahlung

Entscheidet sich das Opfer zur Zahlung, erfolgt die Überweisung entsprechend den Anweisungen – in der Regel in Bitcoin oder einer anderen Kryptowährung.

Ransomware-Statistiken und Trends 2022–2025

Ransomware-Angriffe haben zwischen 2022 und 2023 starke Schwankungen und klare Trends gezeigt – mit ersten Anzeichen für eine weitere Eskalation im Jahr 2024. Im Folgenden finden Sie einen detaillierten Überblick über die wichtigsten Kennzahlen und Entwicklungen rund um Ransomware-Angriffe in diesem Zeitraum.

Gesamtzahl der Angriffe:

2022 2.662 Angriffe
2023 4.611 Angriffe

Durchschnittliche Lösegeldzahlung ($):

2022 457 Mio. US-Dollar
2023 1 Mrd. US-Dollar

Anteil betroffener Unternehmen (ca.):

2022 70%
2023 85%

Cyberangriffe führen zu Datenverlust

Der Bericht „Data Health Check 2023“ zeigt: Cyberangriffe waren die Hauptursache für IT-Ausfälle und Datenverluste – noch vor Hardwaredefekten. Viele Unternehmen überschätzten ihre Vorbereitung: **62 % glaubten, sie könnten ohne ihre IT maximal einen Tag überleben**.
Diese Fehleinschätzung führte zu schwerwiegenden Folgen – vor allem, wenn Backups im Ernstfall nicht funktionierten.

Langfristige Auswirkungen von Datenverlust

Datenverlust hat langfristige Folgen für Unternehmen. **Statistiken zeigen, dass 51 % der Unternehmen innerhalb von zwei Jahren nach einem schweren Datenverlust schließen – und 43 % nie wieder öffnen**. Kleine Unternehmen sind besonders betroffen: **Fast 70 % schließen bereits im ersten Jahr nach dem Vorfall**. Das unterstreicht die Bedeutung robuster und verlässlicher Backup- und Wiederherstellungslösungen.

Ransomware-Ausblick 2025

Ransomware-Angriffe werden 2025 noch ausgefeilter – mit Fokus auf Schwachstellen in Cloud- und VPN-Infrastrukturen sowie Doppel-Erpressung. Das Modell **Ransomware-as-a-Service (RaaS)** verbreitet leistungsfähige Angriffstools weiter und erhöht Anzahl und Vielfalt der Angriffe. Angreifer nutzen weiterhin die Anonymität von Kryptowährungen aus. **Künstliche Intelligenz wird zunehmend für gezielte Phishing- und Ransomware-Kampagnen eingesetzt** – was die Abwehr deutlich erschwert.

Quellen: Statista, Security Magazine, TrueList, Invenio IT, TechRadar

Zentrale Trends und Beobachtungen

- **Strategiewechsel bei der Zielauswahl:** Ransomware-Gruppen setzen verstärkt auf „Big Game Hunting“ – wenige, aber lukrativere Ziele. Die Lösegeldforderungen übersteigen dabei oft **1 Million US-Dollar.**
- **Branchenspezifische Schwachstellen:** 2023 besonders betroffen: **Gesundheitssektor** – wegen der Dringlichkeit von IT-Verfügbarkeit bei lebenswichtigen Diensten. Weitere Zielbranchen: Bildung, Verwaltung, Unternehmensservices.
- **Geografische Auswirkung: USA waren 2023 am stärksten betroffen** – allein im zweiten Quartal wurden **574 Opfer gemeldet.**
- **Wiederholte Angriffe: 80 % der Unternehmen, die gezahlt haben, wurden erneut angegriffen**. Deutliches Zeichen für anhaltende Verwundbarkeit trotz „erfolgter Zahlung“.
- **Zunahme neuer Angreifergruppen:** 2023 wurden **17 % aller Vorfälle** neuen Gruppen zugeschrieben – die Bedrohungslage wird unübersichtlicher. Oft spielt auch **menschliches Fehlverhalten** eine zentrale Rolle bei erfolgreichen Angriffen.

Zentrale Herausforderungen beim Schutz vor Ransomware

Angriffsmethoden und -strategien

Fortschrittliche Verschlüsselungstechniken

- **Ursache:** Moderne Ransomware nutzt starke Verschlüsselungsverfahren wie AES (Advanced Encryption Standard) und RSA (Rivest-Shamir-Adleman). Diese Algorithmen machen es nahezu unmöglich, verschlüsselte Dateien ohne den Schlüssel des Angreifers zu entschlüsseln. Ist eine Datei erst einmal gesperrt, bleibt nur noch die Zahlung als Ausweg – genau das macht diese Technik so gefährlich.
- **Beispiel: Cryptolocker** – eine der ersten Ransomware-Varianten mit starker RSA-2048-Verschlüsselung – setzte einen Standard für künftige Angriffe.
- **Lösung:** Einsatz von Snapshots zur Wiederherstellung betroffener Datenstände.

Ausnutzung von Zero-Day-Schwachstellen

- **Ursache:** Ransomware nutzt häufig sogenannte Zero-Day-Schwachstellen – bisher unbekannte Sicherheitslücken in Software, die von Angreifern ausgenutzt werden, bevor Hersteller ein Sicherheitsupdate bereitstellen können. So lassen sich herkömmliche Schutzmaßnahmen umgehen und Systeme unbemerkt infizieren.
- **Beispiel:** WannaCry nutzte die EternalBlue-Sicherheitslücke in Microsoft Windows, die als Zero-Day-Exploit massive Verbreitung ermöglichte.
- **Lösung:** Regelmäßige und lückenlose Sicherheitsupdates auf allen Ebenen.

Raffinierte Verbreitungsmethoden

- **Ursache:** Angreifer setzen auf ausgeklügelte Verbreitungswege wie Spear-Phishing, Drive-by-Downloads oder manipulierte Werbeanzeigen (Malvertising), um ihre Schadsoftware zu platzieren – oft so gestaltet, dass sie vertrauenswürdig wirkt und gängige Sicherheitslösungen umgeht.
- **Beispiel:** Phishing-E-Mails, die scheinbar von bekannten oder internen Absendern stammen und infizierte Anhänge oder Links enthalten.
- **Lösung:** Hochwertige, mehrschichtige Sicherheitslösungen mit effektiver E-Mail-Filterung und Endgeräteschutz.

Typische Schwachstellen und Angriffsvektoren

Phishing-E-Mails, Sicherheitsprotokolle und Risikobewusstsein

- **Ursache:** Phishing ist eine der häufigsten Methoden zur Verbreitung von Ransomware. Angreifer verschicken E-Mails, die seriös erscheinen, und verleiten die Empfänger dazu, auf schadhafte Links zu klicken oder infizierte Anhänge zu öffnen.
- **Beispiel:** Die Locky-Ransomware wurde häufig über E-Mails mit Word-Dokumenten und schadhaften Makros verbreitet.
- **Lösung:** Mitarbeiterschulungen zum Sicherheitsbewusstsein und eine korrekte Konfiguration der Firewall.

Ungepatchte Softwareschwachstellen

- **Ursache:** Ransomware nutzt Schwachstellen in nicht aktualisierter Software aus, um sich Zugang zu Systemen zu verschaffen. Aktuelle Softwareupdates sind entscheidend, um solche Exploits zu verhindern.
- **Beispiel:** Der NotPetya-Angriff nutzte eine bekannte Schwachstelle im Windows-SMB-Protokoll – obwohl ein Patch bereits verfügbar war, blieb er in vielen Systemen ungenutzt.
- **Lösung:** Regelmäßige Updates und der Einsatz heterogener Systemlandschaften.

Remote Desktop Protocol (RDP)

- **Ursache:** Unsichere RDP-Konfigurationen und schwache Zugangsdaten ermöglichen es Angreifern, sich Zugriff auf Systeme zu verschaffen und Ransomware zu platzieren.
- **Beispiel:** Die Dharma-Ransomware nutzt Brute-Force-Angriffe auf RDP, um sich Zugang zu verschaffen und Schadsoftware auszuführen.
- **Lösung:** Starke RDP-Absicherung oder Nutzung alternativer Fernzugriffslösungen.

Schwachstellen im Datenschutz

Unzureichende Snapshot-Strategien

- **Ursache:** Fehlende oder nicht regelmäßig erstellte Snapshots können im Fall eines Ransomware-Angriffs zu erheblichem Datenverlust führen – insbesondere wenn kritische Dateien verschlüsselt werden.
- **Beispiel:** Unternehmen, die von Ransomware wie CryptoWall betroffen sind und keine unveränderlichen Snapshots nutzen, haben oft keine andere Wahl, als zu zahlen oder ihre Daten zu verlieren.
- **Lösung:** Integration von Snapshots in die Backup-Strategie mit individuellen Aufbewahrungsrichtlinien. Dies erhöht die Datensicherheit, verbessert die Verfügbarkeit und verkürzt die Wiederherstellungszeiten.

Fehlende Datenverschlüsselung

- **Ursache:** Wird vertrauliche Information nicht verschlüsselt, kann dies die Auswirkungen eines Angriffs erheblich verstärken – Angreifer drohen in solchen Fällen mit Veröffentlichung der Daten.
- **Beispiel:** Die Maze-Ransomware kombiniert Dateiverschlüsselung mit Datendiebstahl und erhöht so den Druck auf die Opfer, das Lösegeld zu zahlen.
- **Lösung:** Einsatz von SEDs (Self-Encrypting Drives) und anderen Verschlüsselungsverfahren zur Absicherung sensibler Daten.

Häufige Fehler bei Datensicherung und -wiederherstellung

Im Bereich des Ransomware-Schutzes ist jeder Vorfall einzigartig – abhängig von Branche und Unternehmensstruktur. **Basierend auf unseren Erfahrungen lassen sich jedoch typische Fehler im Bereich Datensicherung identifizieren, die Cyberkriminellen Angriffsflächen bieten.**

Überblick über häufige Fehler basierend auf Open-E-Erkenntnissen

Ausschließliche Abhängigkeit von Backups

Wer sich allein auf Backups verlässt – ohne schreibgeschützte Snapshots – ist anfällig für Ransomware. Snapshots bieten Echtzeit-Kopien im Metadatenformat und ermöglichen die schnelle Wiederherstellung eines sauberen Zustands nach einem Angriff. Sie verhindern die Weiterverbreitung von Ransomware und sorgen für Datenkonsistenz sowie schnellere, effizientere Wiederherstellungsprozesse.

Snapshots nicht regelmäßig testen

Ein häufiger Fehler ist das fehlende Testen von Snapshots. Viele Organisationen gehen davon aus, dass ihre Backups korrekt funktionieren, ohne dies aktiv zu überprüfen. Regelmäßige Tests sind entscheidend, um z. B. beschädigte Backup-Dateien oder unvollständige Datensätze rechtzeitig zu erkennen – bevor ein Ernstfall eintritt. Ohne diese Tests besteht das Risiko, dass Backups genau dann versagen, wenn sie am dringendsten benötigt werden – mit potenziell gravierenden Ausfällen und Datenverlusten.

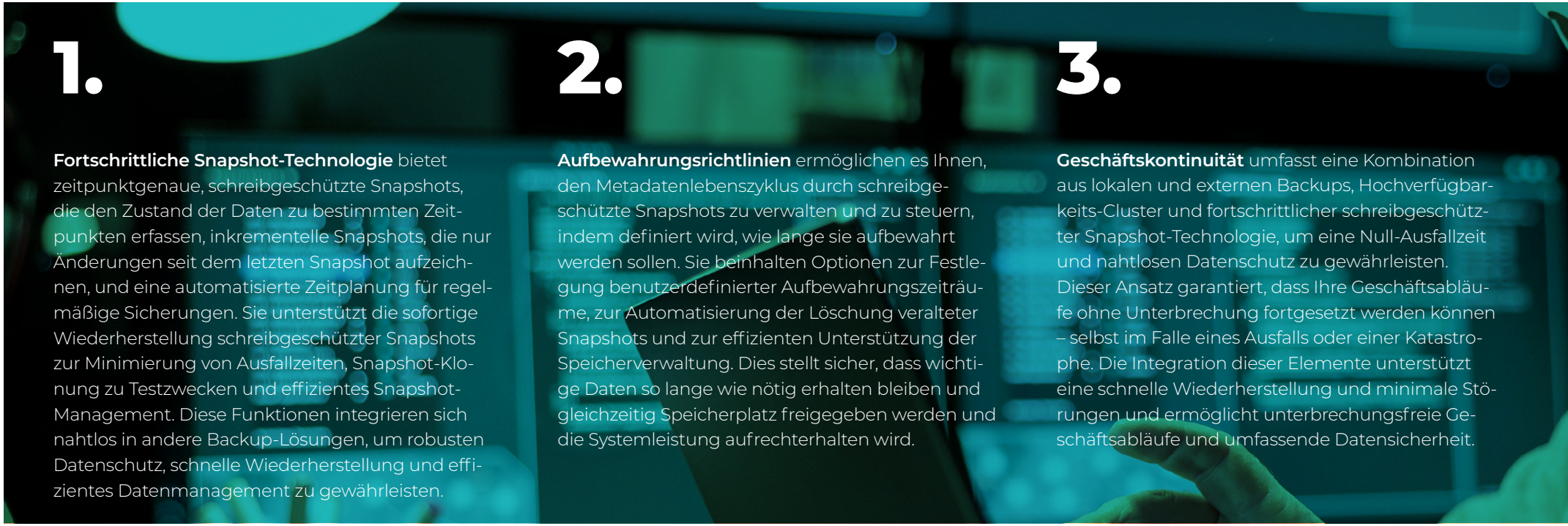
Fehlende Verschlüsselung von Backups

Unverschlüsselte Backups sind ein hohes Sicherheitsrisiko: Sie können bei einem Angriff abgegriffen und ausgelesen werden. Backup-Daten – egal ob lokal, extern oder in der Cloud gespeichert – sollten stets verschlüsselt werden, um vertrauliche Inhalte zu schützen. Selbst wenn ein Backup abgefangen wird, bleibt es damit unlesbar und sicher, und die Vertraulichkeit sowie Integrität der Daten bleiben gewahrt.

Open-E: Profi-Tipps zur Vermeidung von Ransomware-Folgen

Mehrstufige Sicherheitsansätze

Der Einsatz eines mehrschichtigen Ansatzes – einschließlich Firewalls, Antivirensoftware und Intrusion-Detection-Systemen – erhöht die allgemeine Sicherheit und reduziert das Risiko von Ransomware-Angriffen. Open-E JovianDSS ist eine robuste Softwarelösung für Datenspeicherung, die hohe Verfügbarkeit, Datenintegrität und effizientes Datenmanagement bietet. Zu den wichtigsten Funktionen gehören:



1.

Fortschrittliche Snapshot-Technologie bietet zeitpunktgenaue, schreibgeschützte Snapshots, die den Zustand der Daten zu bestimmten Zeitpunkten erfassen, inkrementelle Snapshots, die nur Änderungen seit dem letzten Snapshot aufzeichnen, und eine automatisierte Zeitplanung für regelmäßige Sicherungen. Sie unterstützt die sofortige Wiederherstellung schreibgeschützter Snapshots zur Minimierung von Ausfallzeiten, Snapshot-Klonung zu Testzwecken und effizientes Snapshot-Management. Diese Funktionen integrieren sich nahtlos in andere Backup-Lösungen, um robusten Datenschutz, schnelle Wiederherstellung und effizientes Datenmanagement zu gewährleisten.

2.

Aufbewahrungsrichtlinien ermöglichen es Ihnen, den Metadatenlebenszyklus durch schreibgeschützte Snapshots zu verwalten und zu steuern, indem definiert wird, wie lange sie aufbewahrt werden sollen. Sie beinhalten Optionen zur Festlegung benutzerdefinierter Aufbewahrungszeiträume, zur Automatisierung der Löschung veralteter Snapshots und zur effizienten Unterstützung der Speicherverwaltung. Dies stellt sicher, dass wichtige Daten so lange wie nötig erhalten bleiben und gleichzeitig Speicherplatz freigegeben werden und die Systemleistung aufrechterhalten wird.

3.

Geschäftskontinuität umfasst eine Kombination aus lokalen und externen Backups, Hochverfügbarkeits-Cluster und fortschrittlicher schreibgeschützter Snapshot-Technologie, um eine Null-Ausfallzeit und nahtlosen Datenschutz zu gewährleisten. Dieser Ansatz garantiert, dass Ihre Geschäftsabläufe ohne Unterbrechung fortgesetzt werden können – selbst im Falle eines Ausfalls oder einer Katastrophe. Die Integration dieser Elemente unterstützt eine schnelle Wiederherstellung und minimale Störungen und ermöglicht unterbrechungsfreie Geschäftsabläufe und umfassende Datensicherheit.

4.

Disaster Recovery-Lösungen bieten umfassenden Schutz, indem sie eine schnelle Wiederherstellung nach katastrophalen Ereignissen ermöglichen. Sie beinhalten automatisierte Failover- und Failback-Prozesse, um den Betrieb nahtlos zwischen primären und sekundären Systemen umzuschalten. Die Lösung unterstützt die Echtzeit-Datenreplikation an externe Standorte und gewährleistet damit Datenkonsistenz und minimalen Datenverlust. Durch automatisierte Tests und Validierungen können Sie sicherstellen, dass Ihre Wiederherstellungspläne zuverlässig funktionieren. Dieser Ansatz garantiert minimale Ausfallzeiten und eine schnelle Wiederherstellung von Diensten – und sichert so die Geschäftskontinuität im Katastrophenfall.

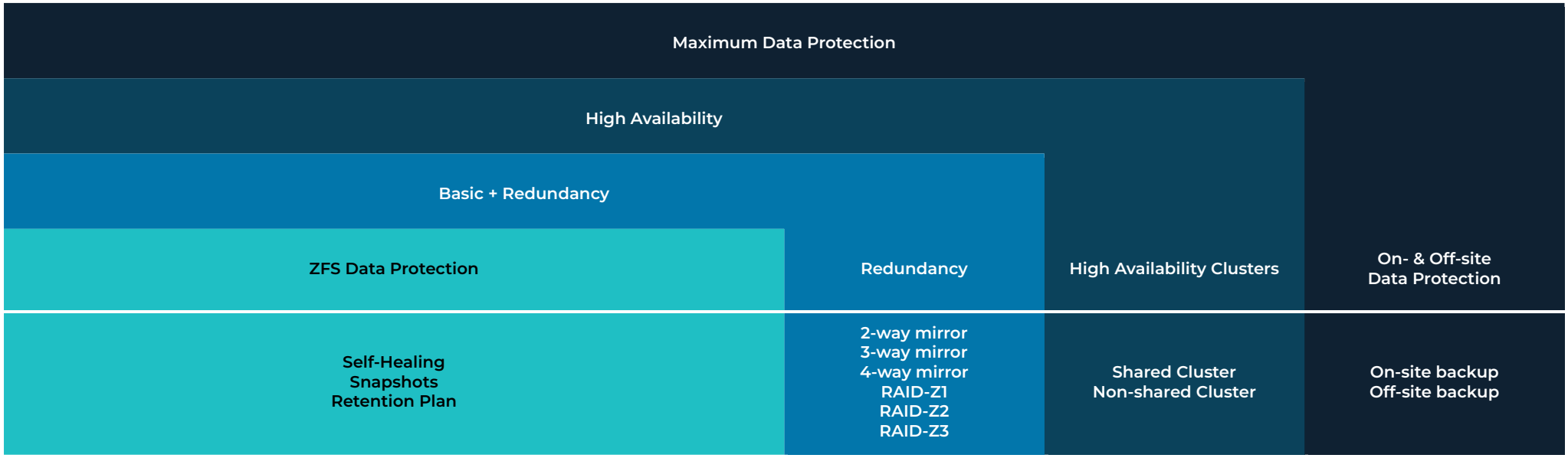
5.

Verschlüsselungstechniken: Open-E JovianDSS unterstützt selbstverschlüsselnde Laufwerke (SEDs), die hardwarebasierte Verschlüsselung bieten. Diese verschlüsseln und entschlüsseln Daten automatisch, ohne die Systemleistung zu beeinträchtigen. Die SED-Funktion sorgt dafür, dass selbst bei physischem Diebstahl von Laufwerken die Daten ohne Authentifizierung unzugänglich bleiben – und stellt so eine zusätzliche Sicherheitsschicht gegen physische Datenpannen dar, die den Ransomware-Schutz ergänzt. Obwohl Verschlüsselung allein Ransomware-Angriffe nicht verhindert, sorgt sie dafür, dass gestohlene Daten nicht gelesen werden können. In Kombination mit weiteren Sicherheitsmaßnahmen wie Firewalls, Antivirensoftware und Intrusion-Detection-Systemen stärkt diese Verschlüsselung die gesamte Sicherheitsstruktur und verbessert den Schutz vor Ransomware.

Sicherheitsfunktionen von Open-E JovianDSS zum Schutz vor Ransomware-Folgen

Ransomware-sichere Daten-Sicherheitsstufen

Die Anforderungen eines Unternehmens bestimmen, welche Business-Continuity-Maßnahmen in der Speicherinfrastruktur notwendig sind. **Bevor Sie verschiedene Funktionen zur Datenspeicherung auswählen, ist es entscheidend, die potenziellen Risiken zu verstehen und alle Details der Infrastruktur zu kennen**. Beginnen Sie mit einer Analyse, wie und warum Ihr Unternehmen Daten speichert, und dokumentieren Sie dann alle Geschäftsprozesse im Zusammenhang mit Datenspeicherung – für ein umfassendes Verständnis der Anforderungen an das Datenmanagement.



Basic ZFS Data Protection

Zum Schutz Ihrer Daten vor Cyberangriffen, stiller Datenkorruption und menschlichen Fehlern ist der Einsatz von ZFS-basierter Software mit Self-Healing-Funktionen entscheidend. Diese Funktionen verringern das Risiko von Datenbeschädigungen und ermöglichen mit Snapshots die Wiederherstellung auf einen früheren Systemzustand – z. B. nach Sicherheitsvorfällen, versehentlichen Löschungen oder Modifikationen.

+ **Schnelle Wiederherstellung mit Snapshots**
+ **Aufbewahrungsrichtlinien**
+ **Self-Healing**

ZFS Data Protection mit Daten-Redundanz

Durch den Einsatz von Snapshots, Self-Healing und RAID-Konfigurationen können Sie Ihre Daten wirksam vor Ransomware, stiller Datenkorruption und Laufwerksausfällen schützen. RAID sorgt für Redundanz und ermöglicht die Wiederherstellung verlorener Daten über Paritätsinformationen – und erhöht so die Ausfallsicherheit Ihrer Speicherlösung.

+ **Basis-Datenschutz mit ZFS**
+ **Daten-Redundanz – RAID-Wiederherstellung**

High-Availability Cluster

Zur Absicherung gegen Datenverlust durch Serverausfälle setzen Branchen wie Einzelhandel, Hotellerie und KMU auf Hochverfügbarkeits-Cluster mit zwei oder mehr verbundenen Nodes. Diese Cluster können mit Shared- oder Non-Shared-Architekturen betrieben werden und gewährleisten unterbrechungsfreien Datenzugriff – auch im Fall von Ransomware oder Hardwarefehlern.

+ **Basis-Datenschutz mit ZFS**
+ **Daten-Redundanz – RAID-Wiederherstellung**
+ **Hochverfügbarkeits-Cluster – Shared und Non-shared**

Open-E JovianDSS On- & Off-site Data Protection

Die lokale Datensicherung mit Open-E JovianDSS speichert Backups sowohl auf dem Produktionsserver als auch auf einem zweiten lokalen Server, um im Ernstfall eine schnelle Wiederherstellung bei minimalen Ausfallzeiten zu ermöglichen. Die externe Datensicherung ergänzt diesen Schutz durch die Speicherung auf einem entfernten Server – so bleiben die Daten sicher und wiederherstellbar, selbst wenn lokale Systeme durch Ransomware betroffen sind.

+ **Basis-Datenschutz mit ZFS**
+ **Daten-Redundanz – RAID-Wiederherstellung**
+ **On- & Off-site-Datensicherung**

Maximale Datensicherheit

Für maximale Datensicherheit kombinieren Sie mehrere Methoden. Open-E JovianDSS lässt sich mit On- & Off-site-Backups und Hochverfügbarkeits-Clustern kombinieren. Auch wenn die Investition zunächst hoch erscheinen mag, liegt sie deutlich unter den Kosten für Datenverlust oder Lösegeld – teure Hardware ist für effektive Sicherheit nicht zwingend notwendig.

+ **Basis-Datenschutz mit ZFS**
+ **Daten-Redundanz – RAID-Wiederherstellung**
+ **Hochverfügbarkeits-Cluster – Shared und Non-shared**
+ **On- & Off-site-Datensicherung**

Gegründet im Jahr 1998 ist Open-E ein etablierter Entwickler von IP-basierter Storage-Management-Software. Das Flaggschiff--Produkt **Open-E JovianDSS** ist eine leistungsstarke, mehrfach ausgezeichnete Storage-Lösung, die exzellente Kompatibilität mit Industriestandards bietet. Gleichzeitig zählt sie zu **den einfachsten Lösungen in Bedienung und Verwaltung** – und gehört zu den **stabilsten und wirtschaftlichsten Systemen am Markt**.

Dank seiner **Zuverlässigkeit, Erfahrung und technischen Kompetenz** ist Open-E für viele führende IT-Unternehmen der **präferierte Technologiepartner**. Open-E kann weltweit auf **über 40.000 Softwareinstallationen verweisen**.

+40000 Software-Installationen weltweit

+120 Länder mit Installationen

+25 Jahre Erfahrung

+800 zertifizierte Techniker & Vertriebsprofis

Open-E, Inc. | +1 (678) 666 2880 (US) | +49 (89) 800777 0 (Europe) | info@open-e.com