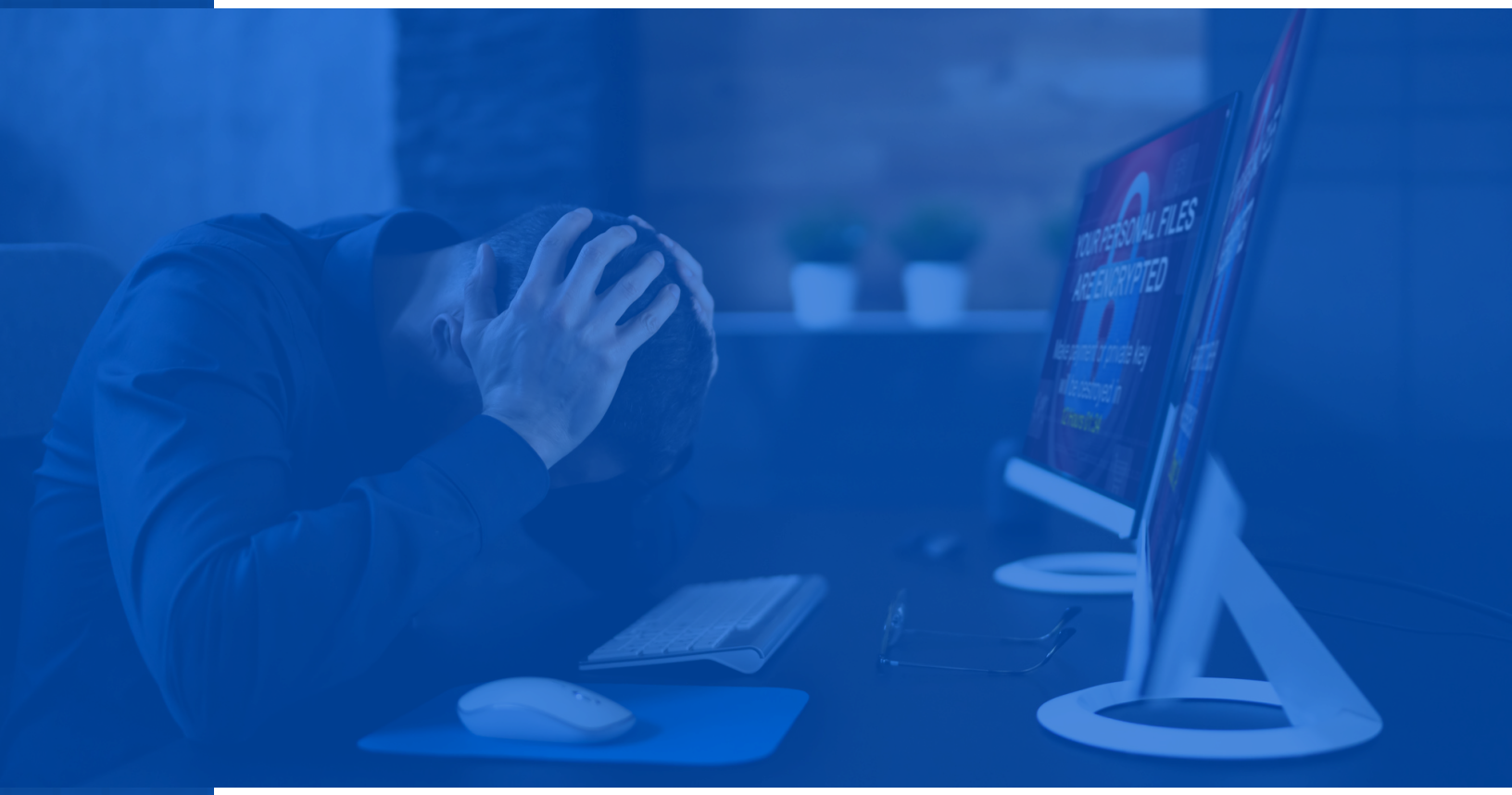
EBOOK

NovaBACKUP



WIE SIE IHRE

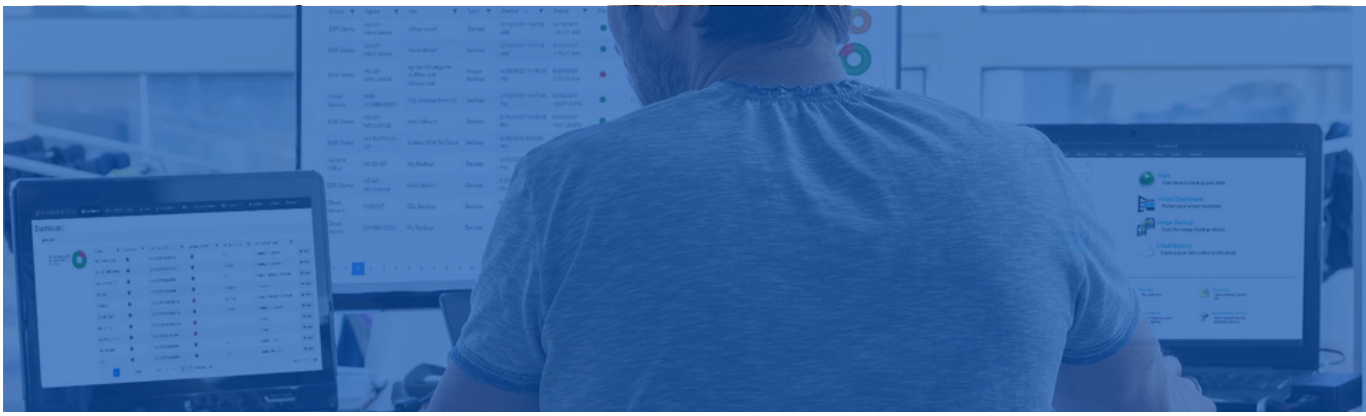
BACKUPS VOR RANSOMWARE SCHÜTZEN

Ein Praxisleitfaden mit NovaBACKUP

Ransomware ist längst kein Einzelfall mehr, sondern ein alltägliches Risiko für Unternehmen aller Größenordnungen – insbesondere für kleine und mittelständische Unternehmen. Angreifer nutzen heute Automatisierung und KI, um sowohl die Anzahl als auch die Raffinesse ihrer Angriffe zu steigern, sodass herkömmliche Abwehrmaßnahmen kaum noch Schritt halten können.

> Im Jahr 2023 waren weltweit über 72% der Unternehmen von Ransomware-Angriffen betroffen.[1] Besonders kleine und mittelständische Unternehmen werden fast viermal so häufig angegriffen wie große Organisationen.[2]

Auch wenn Endpunkt- und Netzwerksicherheit unverzichtbar bleiben, stellen Backups im Ernstfall Ihre letzte Verteidigungslinie gegen Ransomware dar. Werden Ihre Backup-Daten kompromittiert – verschlüsselt, gelöscht oder anderweitig unbrauchbar gemacht – ist eine Wiederherstellung in der Regel nur noch durch Zahlung eines Lösegelds möglich. Aber selbst das ist jedoch oft unzuverlässig und wirkungslos.



Dieser Leitfaden konzentriert sich speziell darauf, wie Sie Ihre Backups vor Ransomware schützen. Wir zeigen praxisnahe Strategien, technische Konfigurationsbeispiele in NovaBACKUP und betriebliche Best Practices, damit Ihre Backups auch bei fortschrittlichen Angriffen widerstandsfähig und wiederherstellbar bleiben.

WARUM DER SCHUTZ VON BACKUPS VOR RANSOMWARE WICHTIG IST

Backups sind oft die letzte Rettung, wenn Ransomware zuschlägt. Doch moderne Ransomware nimmt gezielt Backup-Dateien und -Speicher ins Visier, um eine Wiederherstellung zu verhindern. Der Schutz Ihrer Backups wird daher immer wichtiger. Mit intakten und wiederherstellbaren Backups gelang es Unternehmen, den Betrieb innerhalb einer Woche wiederherzustellen. Viele andere, die von Ransomware betroffen waren, hatten dagegen mit langen Ausfallzeiten zu kämpfen.

> 31% der Unternehmen benötigten zwischen einem und sechs Monaten, um sich von einem Ransomware-Angriff zu erholen, nachdem sie das Lösegeld gezahlt hatten. Im Gegensatz dazu erholten sich 45% der Unternehmen, die Backups verwendeten, innerhalb einer Woche.[3]

Sind sowohl Ihre Produktionsdaten als auch Ihre Backups verschlüsselt oder gelöscht, ist Ihr Sicherheitsnetz weg. Lösegeld zu zahlen ist teuer und unsicher. Selbst nach Zahlung gibt es keine Garantie auf Datenwiederherstellung, und der Prozess zieht sich oft über Monate hinweg.

> Nur 54% der Unternehmen, die Lösegeld zahlten, konnten ihre Daten tatsächlich wiederherstellen.[4]

Saubere, wiederherstellbare Backups sind die einzige Garantie für Geschäftskontinuität. Sie ermöglichen es, Ausfallzeiten zu reduzieren und schwerwiegenden Datenverlust zu vermeiden.

GRUNDLAGEN FÜR EINE RESILIENTE BACKUP-STRATEGIE

Regelmäßige Backups von Dateien und Systemen reichen heute nicht mehr aus. Backups benötigen genauso viel Aufmerksamkeit wie Ihre Produktivsysteme. Die nachstehenden Leitlinien sind die Basis einer robusten Backup-Strategie, mit der Sie kritische Daten schützen und die Geschäftskontinuität selbst bei Angriffen gewährleisten.

1 Mehrere Kopien, inklusive Offsite- und Air-Gap-Backups

Bewahren Sie mindestens drei Kopien Ihrer Daten auf. Die erste „Kopie“ sind Ihre Primärdaten in der Produktionsumgebung. Zusätzlich empfiehlt es sich:

- **Kopien auf lokalem Speicher zu erstellen:** Lokale Backups sind oft das erste Ziel von Ransomware, da sie in der Regel direkt ans Netzwerk angebunden sind. Sie bieten jedoch den Vorteil, dass Daten im Notfall zügig wiederhergestellt werden können.

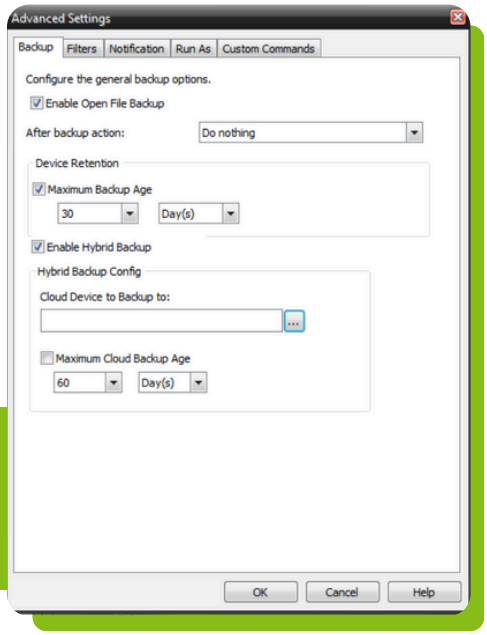
- **Kopien auf externem oder Air-Gap-Speicher zu sichern:** Dazu zählen Cloud-Speicher oder Wechseldatenträger, die nicht dauerhaft mit dem Netzwerk verbunden sind. Besonders Cloud-Backups sind ein wichtiger Bestandteil einer Ransomware-resistenten Strategie, da sie Daten vom Netzwerk isolieren und so eine Wiederherstellung auch bei Ausbreitung der Ransomware ermöglichen. Die richtige Konfiguration ist dabei entscheidend (siehe Punkt 4).

Mit NovaBACKUP:

Hybride Backup-Jobs und optimierte Wiederherstellung

NovaBACKUP automatisiert hybride Backup-Jobs und sorgt dafür, dass sowohl lokale als auch Cloud-Kopien stets aktuell gehalten werden.

Erstellen Sie einen lokalen Backup-Job mit 30 Tagen Aufbewahrung. Aktivieren Sie dann die Hybrid-Backup-Funktion und wählen Sie den Cloud-Speicher mit 60 Tagen Aufbewahrung.



Hybride Backups mit gestaffelter Aufbewahrung und einem Incremental-Forever-Backup-Konzept (siehe #2) adressieren das Problem, dass Ransomware oft wochenlang unentdeckt bleibt. Nur die neueste Sicherung zu behalten, birgt das Risiko, infizierte Daten wiederherzustellen. **Versionierung** sorgt für mehrere Wiederherstellungspunkte an verschiedenen Orten, sodass Sie auf einen sauberen Zustand zurücksetzen können.

Ein weiterer Vorteil: Dank hybrider Backups optimiert NovaBACKUP die **Wiederherstellungsgeschwindigkeit**. Bei der Wiederherstellung nutzt NovaBACKUP zunächst die naheliegendste Quelle – in der Regel den lokalen Speicher – und greift nur auf die Cloud zurück, wenn es wirklich notwendig ist.

2 Setzen Sie auf Incremental Forever-Backups

Traditionelle Backup-Methoden – Voll, Inkremental, Differenziell – haben Jahrzehnte lang ihren Zweck erfüllt, stoßen aber in modernen IT-Umgebungen an ihre Grenzen. Sie bringen Herausforderungen wie große Datenmengen, lange Backup-Fenster oder ineffiziente Speichernutzung mit sich.

Mit NovaBACKUP:

Incremental Forever für widerstandsfähige Backups

NovaBACKUPs Incremental Forever-Methode löst diese Probleme. Nach einer initialen Vollsicherung werden nur noch Änderungen gesichert. Alle Inkremente sind miteinander verlinkt, sodass Wiederherstellungen zu jedem Zeitpunkt möglich sind.

Das Ergebnis: Schnellere Backups, effizientere Speichernutzung (oft mit geringeren Kosten) und eine stabile Grundlage für moderne Datensicherung.

Ausführliche Informationen zur Incremental-Forever-Methode von NovaBACKUP erhalten Sie in unserem Blogbeitrag.

3 Setzen Sie auf unveränderliche (immutable) Backups

Immutability bezieht sich meist auf Cloud-Speicherfunktionen, die das Löschen von Daten für einen festgelegten Zeitraum (z. B. 90 Tage) verhindern. Speicherbasierte Immutability (z.B. Wasabi Object Lock) blockiert Lösch- oder Änderungsversuche auf Speicherebene und schützt so effektiv vor Ransomware.

Mit NovaBACKUP:

Job-basierte Immutability plus Integritätsprüfungen

Im Gegensatz zu Lösungen, die auf Speicher von Drittanbietern setzen, bietet NovaBACKUP eine job-basierte Immutability direkt im Backup-Prozess. Daten können während der Aufbewahrungsfrist weder gelöscht noch verändert werden.

Speicherbasierte Immutability bietet eine zusätzliche Sicherheitsebene, aber NovaBACKUPs job-basierte Immutability erreicht das gleiche Ziel: Backup-Daten bleiben bis zum Ablauf der Aufbewahrung geschützt, es sei denn, die Job-Einstellungen werden explizit geändert.

Beispiel: Bei 30 Tagen Aufbewahrung bleiben alle Versionen Ihrer ausgewählten Dateien – inklusive aller Änderungen – für den gesamten Zeitraum erhalten.

Werden Backup-Dateien auf dem Speicher gelöscht oder verändert, erkennt NovaBACKUP dies durch eingebaute Prüfmechanismen. Zu Beginn jedes Backup-Jobs wird die Integrität aller Backup-Dateien (lokal und in der Cloud) sowie der lokal gespeicherten Indizes geprüft. Fehlt eine Datei oder ist sie beschädigt (z. B. durch böswilliges Löschen auf einem NAS), wird sie beim nächsten Backup automatisch erneut gesichert.

4 Backup-Speicher isolieren und Zugriffe kontrollieren

Einer der wichtigsten Aspekte beim Schutz Ihrer Backups vor Ransomware ist die Trennung des Backup-Speichers – sowohl lokal als auch extern – von der Produktionsumgebung. **Backup-Speicher sollte niemals als Netzlaufwerk auf Produktivsystemen eingebunden werden**, und Backup-Ziele sollten ausschließlich für Backup-Daten verwendet werden, nicht für Dateifreigaben, Zusammenarbeit oder Produktivdaten.

Backup-Speicher sollte nur vom Backup-Server oder -Agent erreichbar sein, nicht von anderen Rechnern im Netzwerk. So verhindern Sie, dass Ransomware über kompromittierte Endpunkte auf Backup-Dateien zugreift.

Vermeiden Sie es, Backups auf Diensten wie OneDrive oder Google Drive zu speichern, da diese oft in den täglichen Workflow eingebunden sind. So verringern Sie das Risiko von versehentlichen Löschungen, Überschreibungen oder Ransomware-Infektionen über synchronisierte Endpunkte.

Erstellen Sie außerdem einen dedizierten Backup-Benutzer für alle Backup-Operationen auf Ihrem Backup-Speicher (NAS, USB, Cloud etc.) und setzen Sie das Least-Privilege-Prinzip um.

> Bis zu 95% aller Datenlecks im Jahr 2025 entstanden durch menschliche Fehler. Die Isolierung von Backup-Zugangsdaten minimiert das Risiko versehentlicher Offenlegung. [5]

Mit NovaBACKUP:

Verschlüsselte Zugangsdaten und kontrollierter Zugriff

Bei der Konfiguration des Backup-Speichers in NovaBACKUP werden alle Zugangsdaten verschlüsselt in der Anwendung gespeichert und sind somit nicht für Benutzer oder Endpunkte sichtbar.

Für lokalen Speicher wie ein NAS können Sie einen dedizierten Backup-Benutzer für alle Backup-Operationen zuweisen. NovaBACKUP speichert diese Zugangsdaten verschlüsselt in den Konfigurationsdateien, sodass sie nicht von Ransomware oder unbefugten Nutzern ausgelesen werden können.

Für den integrierten Cloud-Speicher von NovaBACKUP werden Zugangsdaten ausschließlich für Backup-Operationen generiert und verwaltet. Dieser Speicher kann für keinen anderen Zweck genutzt werden, und nur der Backup-Agent hat Zugriff. Unnötige Angriffsflächen werden so eliminiert.

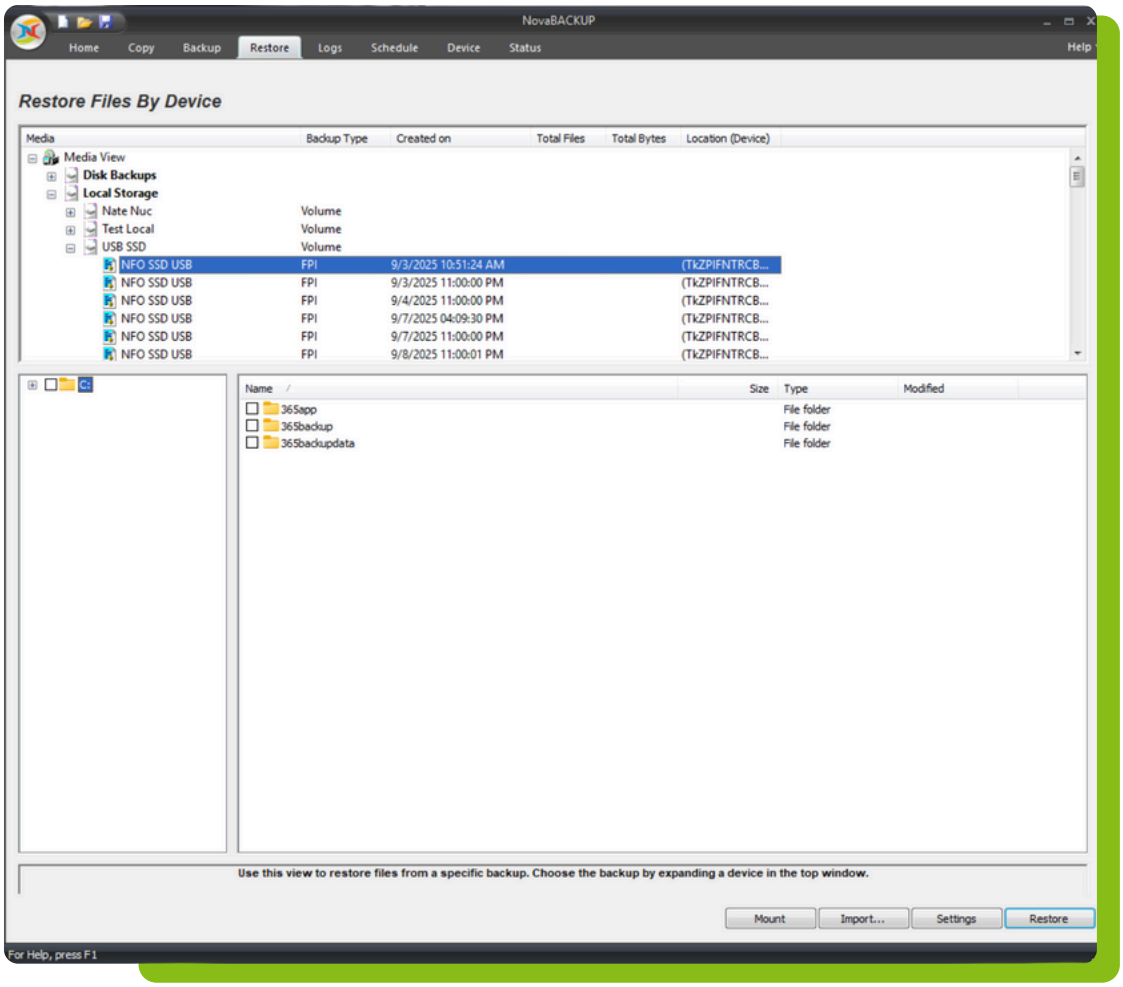
5 Testen Sie Wiederherstellungen und prüfen Sie regelmäßig die Integrität

Backups sind nur dann hilfreich, wenn sie im Bedarfsfall auch erfolgreich wiederhergestellt werden können. Deshalb sind regelmäßige Wiederherstellungstests unerlässlich, um die Datenintegrität zu bestätigen und die Wiederherstellungsgeschwindigkeit zu messen. Verlassen Sie sich nicht nur auf automatische Prüfungen – Fehler passieren. Führen Sie immer auch manuelle Wiederherstellungstests durch. So stellen Sie sicher, dass Sie und Ihr Team wissen, wie eine Wiederherstellung tatsächlich abläuft. Dokumentieren Sie außerdem Ihre Wiederherstellungsprozesse, damit jedes Teammitglied sie im Ernstfall ausführen kann.

Mit NovaBACKUP:

Integrierte Verifikation und einfache manuelle Prüfungen

Neben der in Punkt 3 beschriebenen integrierten Verifikation können Sie mit NovaBACKUP Backups mounten, um die Integrität manuell zu prüfen. Sie können Dateien durchsuchen und verifizieren, ohne eine vollständige Wiederherstellung durchzuführen. So machen Sie Daten außerdem schnell zugänglich für Ihr Team, während Sie komplette Systeme und Netzwerke wiederherstellen.



BONUS-TIPP

Verschlüsselung ist Pflicht

Auch wenn eine Backup-Verschlüsselung Ransomware nicht daran hindert, Ihre Backup-Dateien zu sperren, stellt sie sicher, dass die darin enthaltenen Daten auch bei Diebstahl oder unbefugtem Zugriff unlesbar bleiben. Verschlüsseln Sie daher immer alle lokalen und Cloud-Backups – sowohl bei der Sicherung als auch bei der Übertragung, um unbefugten Zugriff zu verhindern.

FAZIT

Ein wirksamer Schutz von Backups vor Ransomware erfordert eine kontinuierliche Weiterentwicklung der Backup-Strategie. Es gibt keine einzelne Einstellung, die vollständigen Schutz garantiert. Entscheidend ist das Zusammenspiel aus Funktionen, Strategie und laufender Betreuung. Dazu gehören auch regelmäßige Kontrollen von Konfigurationen, Aufbewahrungsrichtlinien und Zugriffsrechten.

Ebenso wichtig: Testen Sie Wiederherstellungen regelmäßig, um die Datenintegrität zu prüfen und sicherzustellen, dass Wiederherstellungsprozesse dokumentiert und von jedem Teammitglied ausführbar sind.

Warten Sie nicht, bis ein Vorfall Schwachstellen in Ihrer Backup-Isolation oder Ihrem Wiederherstellungsprozess aufdeckt. Handeln Sie jetzt: Überprüfen Sie Ihre Backup-Jobs, kontrollieren Sie die Aufbewahrung und Versionierung und stellen Sie sicher, dass sowohl lokale als auch Cloud-Backups geschützt und wiederherstellbar sind.

Sind Sie bereit, Ihre Backup-Strategie zu verbessern?
Testen Sie NovaBACKUP kostenlos oder vereinbaren Sie eine Expertenanalyse Ihrer aktuellen Konfiguration.

ÜBER NOVABACKUP

Die NovaBACKUP Europe GmbH ist spezialisiert auf Backup und Disaster Recovery für Reseller und Managed Service Provider mit Fokus auf die Betreuung stark regulierter, professioneller Branchen. Mit über einer Million geschützten Maschinen und über zwanzig Jahren auf dem Markt, ist es das Ziel von NovaBACKUP, weltweit leistungsstarken, zuverlässigen und erschwinglichen Datenschutz zu bieten.

Sprechen Sie noch heute mit einem unserer Backup-Experten für eine kostenlose Beratung zu Ihrer Backup-Umgebung.

Unser Service-Versprechen

Wir versprechen Ihnen, den Schutz und die Sicherheit Ihrer Daten so zu behandeln, als wären es unsere eigenen. Unser Ziel ist es, die Datensicherung so einfach und zuverlässig wie möglich zu gestalten. Sie können sich darauf verlassen, dass wir Sie professionell und fachkundig unterstützen, um Ihren Anforderungen an Ihre Datensicherung gerecht zu werden. Wenden Sie sich an unser Team, wenn Sie Unterstützung bei der Datensicherung und -wiederherstellung benötigen.

NovaBACKUP

QUELLEN:

1 https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

2 https://www.verizon.com/business/resources/reports/dbir/

3 https://www.sophos.com/en-us/content/state-of-ransomware

4 https://securitybuzz.com/cybersecurity-news/ransomwares-dirty-secret-paying-doesnt-guarantee-recovery/

5 https://www.mimecast.com/resources/ebooks/state-of-human-risk-2025/

NovaBACKUP Europe GmbH
Marienstrasse 89, 30171 Hannover,
Deutschland

Tel.: +49 (40) 80811371

Email: kontakt@novabackup.de

www.novabackup.de