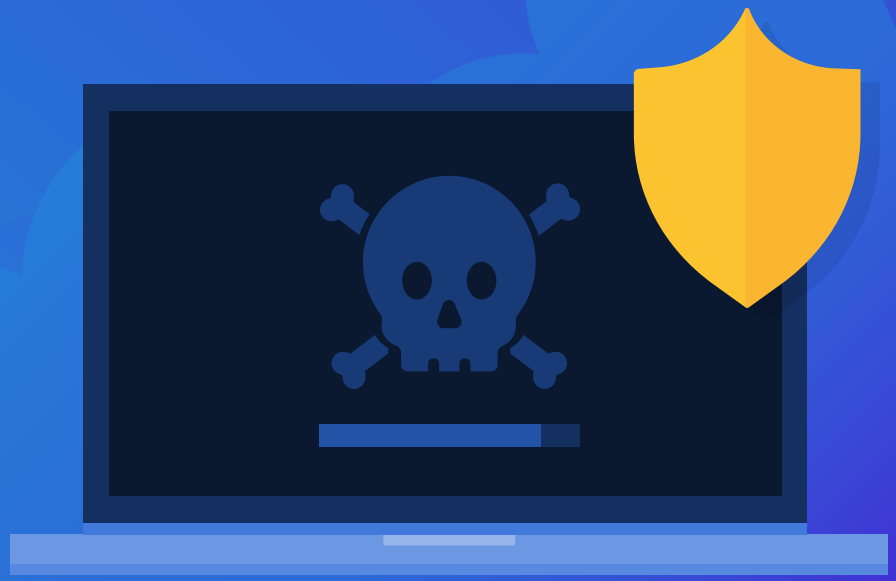
E-Book

datto

# **Backup in Gefahr:** Schutz für Ihre letzte Verteidigungslinie



## Einführung

Im Jahr 2020 entfielen 28 %[1] aller Cyberangriffe auf kleine und mittlere Unternehmen. Hacker suchen nach Schwachstellen in Netzwerken, Servern und Endstellen, um Ransomware und andere Arten von Malware zu verbreiten, Benutzerdaten zu stehlen und sonstiges Unheil anzurichten. Dem Verizon 2020 Data Breach Investigations Report, zufolge, den Sie hier finden, lassen sich im Hinblick auf Verluste und Angriffe Unterschiede zwischen KMU (weniger als 1.000 Mitarbeiter) und größeren Unternehmen (mehr als 1.000 Mitarbeiter) feststellen. Und der größte Unterschied besteht darin, dass die Wahrscheinlichkeit eines Malware-Angriffs bei KMU doppelt so hoch ist.

Der Fokus dieses Schriftstücks liegt auf dem Backup, einer Komponente der Business Continuity und Disaster Recovery (BCDR). Warum Backups? Weil das Backup Ihre letzte Verteidigungslinie ist. Wenn ein Server mit Ransomware infiziert ist oder kritische Dateien versehentlich gelöscht werden, brauchen Sie ein Backup, auf das Sie zurückgreifen können, um die Wiederherstellung vorzunehmen. Aber nicht alle Backups werden auf die gleiche Weise erstellt. So können beispielsweise die Zeiträume für die Wiederherstellung massiv variieren – je nachdem, mit welcher Lösung Sie arbeiten. Und schlimmer noch: Auch Ihre Backups können von Hackern angegriffen werden. In diesem Schriftstück werden wir einen Blick auf bewährte Methoden werfen, die Ihnen helfen, Ihre Backups zu sichern und einsatzbereit zu halten, damit Sie mit der Wiederherstellung keine Zeit verlieren.

„Angreifer bevorzugen kurze Pfade und lassen sich nur selten auf lange Pfade ein[2]“

## Mögliche Erscheinungsformen von Backup-Attacken

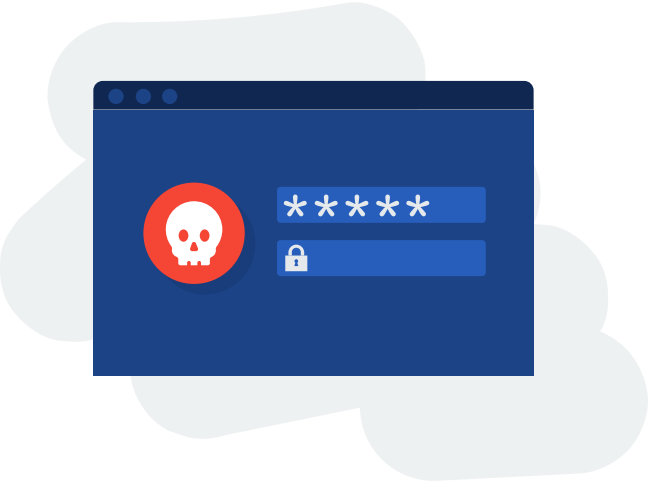
Der Verizon 2020 DBIR Report nutzt die VERIS-Klassifizierung, um die Bedrohungen zu kategorisieren. Dieser Klassifizierung zufolge gibt es folgende Gefahren:

- Malware (Ransomware, Viren, etc.)
- Hacker-Angriffe (gestohlene Anmeldedaten, Hintertüren)
- Soziale Angriffe (Phishing, Pretexting)
- Missbrauch (unerlaubte Nutzung von Privilegien)
- Physische Angriffe (Diebstahl, Manipulation)
- Versehen (Fehlkonfiguration, Falschlieferung, Verlust)
- Umweltbezogene Angriffe (Stromausfall, Witterungsverhältnisse)

Sie alle können die Sicherheit des Backups bedrohen. Dennoch werden wir uns hier auf Hacker-Angriffe, Malware und Versehen konzentrieren. Denn wie aus dem Bericht hervorgeht, **handelte es sich in 45 % der Vorfälle um Hacker-Angriffe, bei 22 % um Versehen und bei 17 % um Malware**. Sehen wir uns jede dieser Bedrohungen einmal einzeln an, betrachten wir die jeweiligen Schwachstellen der Backups und überlegen wir, wie Sie die Risiken mindern können.

### Hacker-Angriffe:

Der Definition zufolge ist ein Hacker ein böswilliger Akteur, der in Computersystemen, Anwendungen und Netzwerken nach Schwachstellen sucht, über die er die entsprechenden Systeme beeinträchtigen und/oder Daten stehlen kann. Bei Backups suchen Hacker zunehmend nach Lücken in der Backup-Software, den Backup-Dateien und den Systemen, in denen die Backup-Daten gespeichert sind.




Hacker versuchen, die Anmeldedaten eines Backup-Administrators zu stehlen, um sich über die Hintertür Zugriff auf die Systeme und Daten zu verschaffen.

**Backup-Software:** Backup-Softwarelösungen erfordern naturgemäß eine hohe Zugriffsebene für Dateien, Systeme, virtuelle Geräte, Datenbanken und andere Aspekte einer IT-Umgebung. Hacker versuchen hier, die Anmeldedaten eines Backup-Administrators zu stehlen, um sich über die Hintertür Zugriff auf die Systeme und Daten zu verschaffen.

Darüber hinaus setzen einige Backup-Produkte eine Konfigurationsdatenbank ein, in denen die Anmeldedaten gespeichert werden, die erforderlich sind, um sich mit den Systemen zu verbinden, deren Backups sie archivieren, Wenn ein Hacker in diese Datenbank eindringt, könnte er sich möglicherweise Zugang zu jedem einzelnen geschützten System verschaffen.

**Backup-Dateien:** Backup-Dateien stellen problemlose Ziele dar – ganz einfach aufgrund ihrer Dateiendung. So ist zum Beispiel eine Datei mit der Benennung .BAK ziemlich leicht zu finden. Hacker könnten sich Zugang zur Backup-Software verschaffen und die Backup-Dateien deaktivieren oder löschen.

**Remote-Zugang:** Da viele Backup-Produkte eine Remote-Verbindung zum Server brauchen, um diesen zu sichern oder Backups zu verwalten, kann die Nutzung einer Authentifizierung per Passwort eine Schwachstelle darstellen, die geschützte Systeme angreifbar macht. Denn Passworte sind sehr leicht zu stehlen. Auch die Tatsache, dass Sie eine Remote Monitoring & Management-Software (RMM) zur Verwaltung der Backups nutzen, kann Angriffsfläche bieten.

**Backup-Verschlüsselung:** Es ist nicht ungewöhnlich, dass Backups verschlüsselt sind. Wenn jedoch ein Angreifer Zugang zu diesem Code erhält, kann er das Backup auslesen und/oder den Code ändern, wodurch Sie selbst den Zugang zu den Daten verlieren. Aus diesem Grunde ist es so wichtig, dass Sie im Hinblick auf den Code für Backup-Verschlüsselungen bewährten Verfahren folgen. Dazu gehört beispielsweise, den Code auf einem separaten Gerät zu speichern, das Gerät physisch zu sichern, etc.

In Anbetracht der Bedeutung, die eine robuste Backup- und Business Continuity-

Wenn die jeweiligen Systemadministratoren nicht wissen, was der andere tut, und der für Backups gedachte Speicherplatz entfernt oder gelöscht wird, haben Sie ein Problem.

Strategie hat, sind verschiedene bewährte Verfahren zu befolgen.

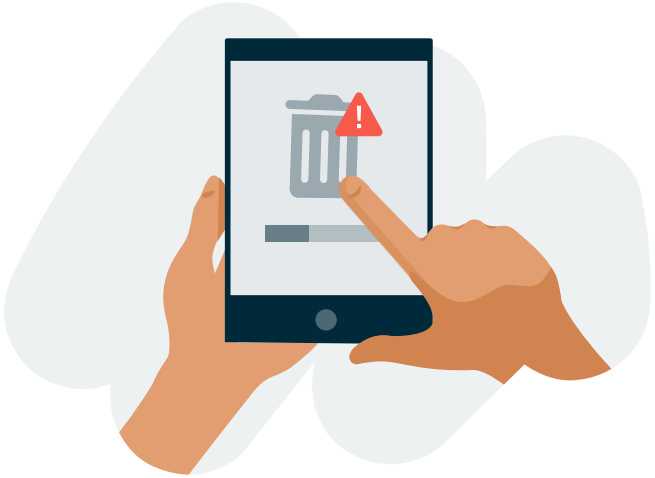
- Nutzen Sie die Zwei-Faktor-Authentifizierung (2FA) für den Zugriff auf das Admin-Portal Ihrer Backup-Software.
- Wenn Sie mit einer Backup-Anwendung arbeiten, stellen Sie sicher, dass Sie sich nicht direkt über eine einfache LAN-Verbindung mit ihr vernetzen können.
- Arbeiten Sie nicht mit Passworten, wenn Sie einen Remote-Zugang nutzen. Greifen Sie stattdessen lieber auf eine SSH-Authentifizierung mit Schlüsselpaaren zurück.
- Wenn Sie zur Verwaltung der Backups ein separates Produkt verwenden, wie etwa ein RMM-Tool, achten Sie darauf, dass auch dieses über 2FA verfügt.
- Stellen Sie sicher, dass Sie die Backup-Kopien an einem sicheren Ort aufbewahren – vorzugsweise geografisch von den primären Daten und Backups getrennt.

## Versehen:

Es hat wohl jeder schon einmal den „Oh-nein!"-Moment erlebt, in dem ihm bewusst wurde, dass er etwas gelöscht hat, was er gar nicht löschen wollte. Im Folgenden finden Sie einige häufig vorkommende Versehen, die sich auf Ihre Möglichkeit einer Wiederherstellung auswirken können.

**Löschen von Backup-Dateien:** Wie bereits erwähnt wurde, sorgt die Dateiendung von Backups dafür, dass sie leicht zu finden sind. Damit wird es für böswillige Akteure zum Kinderspiel, sie zu entdecken. Aber auch ein versehentliches Löschen kann vorkommen. Und da Backup-Dateien groß sind, wird der Platz, den eine solche Datei eingenommen hat, oft schnell von jemand anderem wieder mit Beschlag belegt.

**Stilllegung oder Entfernung von Speicherplatz:** Dies trifft insbesondere für größere IT-Strukturen mit verschiedenen Systemadministratoren zu. Wenn die jeweiligen Systemadministratoren nicht wissen, was der andere tut, und der für Backups gedachte Speicherplatz entfernt oder gelöscht wird, haben Sie ein Problem.



Es hat wohl jeder schon einmal den „Oh-nein!“-Moment erlebt, in dem ihm bewusst wurde, dass er etwas gelöscht hat, was er gar nicht löschen wollte.

**Löschen eines Agent:** Es ist nicht ungewöhnlich, dass Server kommen und gehen, Anwendungen ein Upgrade erhalten oder virtuelle Geräte verschoben, umbenannt oder gelöscht werden. Manchmal wird im Trubel einer solchen Maßnahme auch der Backup-Softwareagent und/oder Eintrag gelöscht, was dazu führt, dass diese Geräte nicht mehr gesichert werden.

**Upgrades:** Der erste Schritt eines jeden Upgrades sollte darin bestehen, dass Sie „vor jeder Änderung ein Backup“ anfertigen“ – aber was ist, wenn das Upgrade die Backup-Lösung selbst betrifft? Viele alte Backup-Produkte stützen sich auf Kataloge oder Verzeichnisse der Daten, die gesichert werden. Wenn diese Kataloge oder Verzeichnisse überschrieben, gelöscht, umbenannt oder anderweitig verändert werden, kann das dazu führen, dass auch die Backups selbst nicht mehr lesbar sind, selbst wenn die Datei an sich noch existiert.

Wie also schützen Sie sich vor dem zweithäufigsten Grund für Datenverluste und der Erkenntnis, dass es Ihre eigene Schuld war, wenn Sie die Backups gelöscht haben?

- **Je mehr Kopien, desto besser.** Moderne Backup-Software bringt nicht die Probleme oder den Mehraufwand mit sich, den alte Lösungen im Hinblick auf Backups bedeuteten. Die meisten modernen Lösungen können verschiedene Zeitpunkte für Wiederherstellungen anbieten, die ganz davon abhängig sind, in welcher Frequenz die Backups vorgenommen werden (beispielsweise alle 5 Minuten oder alle 24 Stunden).
- **Arbeiten Sie mit Zugangskontrollen** für Backup-Dateien und schränken Sie diese so weit wie möglich ein.
- **Vervielfältigen Sie Ihre primären Backups.** Die meisten Wiederherstellungen stützen sich auf ein Backup, das weniger als 48 Stunden alt ist. Deshalb empfiehlt es sich, das neueste Backup zu kopieren und in einer sicheren Cloud oder auf einem anderen Server Ihres Unternehmens zu speichern.
- **Wenn Sie eine Backup-Software haben, die mit Katalogen und Verzeichnissen arbeitet**, achten Sie darauf, diese zu sichern. Außerdem sollten Sie sich nach modernen Backup-Lösungen umsehen, die nicht so leicht korrumpiert werden können.

Die ebenfalls zur Kategorie der Malware gehörende Ransomware befindet sich auf dem Vormarsch und ist mittlerweile die am zweithäufigsten auftretende Malware-Art.

## Malware:

Auch wenn das Vorkommen von Malware insgesamt über die Jahre zurückgegangen ist[3], befindet sich die Ransomware, die ebenfalls zur Kategorie der Malware zählt, deutlich auf dem Vormarsch. Laut des Verizon-Berichts ist sie mittlerweile die am zweithäufigsten eingesetzte Malware-Art.

Ransomware wird üblicherweise über Phishing-E-Mails verbreitet, die den Benutzer dazu bringen, auf einen Link zu klicken oder einen Anhang herunterzuladen, der die Malware in seinem System installiert. Sobald die Ransomware auf einem PC oder Server installiert wurde, beginnt sie damit, nach Dateien zu suchen, die man verschlüsseln kann. Da sich Ransomware still und heimlich ausbreitet, kann durchaus einige Zeit vergehen, bis man ihr Vorhandensein bemerkt.

Wenn die Angreifer der Meinung sind, dass sie die Systeme gründlich infiltriert haben, beginnen sie mit dem Verschlüsseln der Dateien, sodass der Benutzer nicht mehr auf diese zugreifen kann. Wird das geforderte Lösegeld nicht gezahlt, können sie auch gelöscht werden.

**Backup-Dateien:** Wie bereits erwähnt wurde, sind auch Backup-Dateien einfach nur ein weiterer Dateityp, was bedeutet, dass sie ebenso wie alle anderen Dateien von Ransomware verschlüsselt werden können. Wenn Ihre Backups beschädigt werden, gibt es keine Chance mehr auf eine Wiederherstellung. Die einzige Möglichkeit ist dann die Zahlung des Lösegeldes. Und da die Dateiendungen der Backup-Lösungen leicht zu entdecken sind, können Ransomware-Angreifer gezielt nach ihnen suchen und so dafür sorgen, dass das betroffene System nicht wiederhergestellt werden kann.

Ihre Backup-Dateien sind unter Umständen Ihre letzte Verteidigungslinie. Wie also können Sie sie schützen?

Ihre Backup-Dateien sind unter Umständen Ihre letzte Verteidigungslinie. Wie also können Sie sie schützen?

- **Seien Sie proaktiv und prüfen Sie die Dateien beim Backup auf Ransomware.** Bei den meisten modernen Backup-Lösungen ist der Ransomware-Scan ein integraler Bestandteil der Lösung.
- **Bewahren Sie Ihre Backup-Kopien an einem sicheren Ort außerhalb des Netzwerks auf.** Wenn Ihre primären Systeme, einschließlich der (vor Ort befindlichen) lokalen Backups, geschädigt werden, können Sie die betroffenen Systeme dank unberührter Backups, die Sie in einem sicheren, unveränderlichen Cloud-Speicher archiviert hatten, lokal oder in der Cloud wiederherstellen.
- **Je mehr Kopien, desto besser.** Bei modernen Backup-Lösungen sorgen granulare Backups oder „Schnappschüsse" dafür, dass verschiedene Zeitpunkte zur Verfügung stehen, von denen man in Bezug auf eine Wiederherstellung ausgehen kann.
- **Ziehen Sie auch BCDR-Lösungen in Erwägung**, die es Ihnen ermöglichen, den Geschäftsbetrieb lokal oder in der Cloud schnell wiederherzustellen, wenn Ihre primären Systeme Angriffen ausgesetzt waren.

## Zusammenfassung

Ob es sich um Hacker-Angriffe, Malware oder menschliches Versagen handelt – die häufigsten Gründe für Schäden an primären Daten können auch Backups betreffen. Gerissene Angreifer möchten sicherstellen, dass PCs, Server oder virtuelle Geräte nicht wiederhergestellt werden können und richten das Augenmerk daher vermehrt auf Backup-Lösungen.

Erfahren Sie mehr über Datto Unified Continuity →

**Datto Unified Continuity ist eine Business Continuity-Lösung, die vom Server bis zum PC alles abdeckt und dabei die Flexibilität bietet, Daten lokal, direkt in der Cloud oder lokal und in der Cloud zu sichern.** Dies sind die Schlüsselemente von Datto Unified Continuity:

- Umfassender Schutz für Server, virtuelle Geräte, SaaS und PC/Laptops
- Integrierter Ransomware-Scan beim Backup
- 2FA beim Zugriff auf das Datto-Portal, um Backups zu verwalten
- Sichere Backup-Appliances, auf die nicht lokal zugegriffen werden kann
- Sofortige lokale Wiederherstellung
- Datto Cloud für Backup-Speicherung außerhalb des Standorts
  - Sicherer Zugriff mit 2FA und SOC-II-Compliance
  - Geografisch verteilte Datenzentren für Sicherheit und Datensouveränität
  - Optional unbeschränkte Speicherung in der Cloud
  - Verschlüsselte Remote-Vervielfältigung
  - Optionale Verschlüsselung der Backup-Daten
- Sofortige DRaaS-Wiederherstellung in der Datto Cloud
- Exklusive Cloud Deletion Defense™ zum Schutz vor versehentlichem oder böswilligem Löschen von Backups
- Image-basierte Point-in-Time-Recovery

Geschäftsdaten werden an vielen Orten gespeichert - auf Servern, Desktops, Laptops und Cloud-basierten Anwendungen. All dies macht Datto Unified Continuity nicht nur zu Ihrer letzten Verteidigungslinie, sondern auch zu Ihrer stärksten Waffe, wenn Sie Ihre Daten vor Hackern, Versehen und Malware schützen möchten.

---

[1] Verizon 2020 Data Breach Investigations Report
[2] Verizon 2020 Data Breach Investigations Report
[3] Verizon 2020 Data Breach Investigations Report