



## Ransomware Datenrettung

Wenn Schadsoftware in das System eines Unternehmens eindringt und Erpresser Lösegeld verlangen, können die Gesamtauswirkungen - Downtime, Reputation und die Zahlung selbst - großen Schaden anrichten.

Sicherheitsbehörden wie das FBI raten von Lösegeldzahlungen ab. Denn dies fördert das Geschäftsmodell der Cyberkriminellen und bietet dem betroffenen Unternehmen keinerlei Garantie, dass die Daten nach der Zahlung wieder vollständig entschlüsselt werden. Vielmehr bietet sich an, erfahrene Experten hinzuzuziehen, um das beste Vorgehen beim jeweiligen Ransomware-Fall festzulegen.

Schnelle Hilfe durch professionelle Datenrettung.

Ontrack, die globale Marke für Datenrettung von KLDISCOVERY, hat eine Reihe von Tools entwickelt, mit denen Daten nach Ransomware-Angriffen wiederhergestellt werden können - von verschlüsselten Systemen, virtuellen Maschinen, Backup-Dateien, Bändern und anderen Speichermedien. Mit Laboren auf der ganzen Welt, helfen die Datenrettungsingenieure Kunden rund um die Uhr bei Datenrettungen aller Art.

Unsere Experten unterstützen Sie mit speziell entwickelten Tools bei der Datenwiederherstellung nach Ransomware-Angriffen.

Wenn Ihr Unternehmen Opfer eines Ransomware-Angriffs wurde:



- Minimieren Sie sofort die Angriffsfläche, indem Sie die infizierten Rechner vom Netzwerk trennen.
- Kontaktieren Sie uns so früh wie möglich: Unser Team berät Sie kostenlos über Möglichkeiten der Datenwiederherstellung und wie Sie weiterem Datenverlust verhindern können.
- Versuchen Sie nicht die betroffenen Daten selbst zu entschlüsseln; dies könnte zukünftige Wiederherstellungsversuche unmöglich machen.

# Übersicht über den Datenrettungsprozess

Obwohl jeder Ransomware-Vorfall einzigartig und von unterschiedlicher Komplexität ist, können häufig Daten wiederhergestellt werden. Der Erfolg hängt u.a. von der Art des Angriffs, den betroffenen Systemen und den Maßnahmen ab, die bei der Entdeckung ergriffen wurden.



## Beratung

Sofortige telefonische Beratung durch unsere Datenrettungsspezialisten.



## Evaluierung

Evaluierung des Speichermedium, welche Daten wiederhergestellt werden können.



## Wiederherstellung

Die Datenrettung wird von unseren Ingenieuren im Labor durchgeführt.



## Rückversand

Die wiederhergestellten Daten werden auf einem verschlüsselten Medium an den Kunden zurückgesendet.

## Ransomware Fallstudien

- **Phishing Attacke**  
Ein multinationaler Chemiekonzern wurde Opfer eines Ransomware-Angriffs. Ein Server mit Administratorrechten konnte durch Phishing übernommen werden. Die Ransomware formatierte alle Festplatten und erstellte ein neues Aggregat. Ontrack konnte ein Rebuild des RAID-Systems und der ursprünglichen Volumes machen und die Daten des Kunden wiederherstellen.
- **CryptoLocker Ransomware**  
Der Laptop eines einzelnen Benutzers in einem großen Pharmaunternehmen wurde mit der Ransomware CryptoLocker infiziert. Der Laptop war mit dem Unternehmensnetzwerk verbunden, wodurch die Malware 46 Shares infizieren konnte. Durch die Nutzung des proprietären Betriebssystems (OnTap) und Dateisystems (WAFL) von NetApp, waren die Ontrack Techniker in der Lage, kritische Daten aus unverschlüsselten Kopien von vor dem Zeitpunkt des Angriffs zu finden und zu rekonstruieren.
- **Gelöschte Backups**  
Ein Firmenserver wurde von Ransomware angegriffen, die Daten von Microsoft Dynamics 365 verschlüsselt und Lösegeld gefordert. Aktuelle Backups des Servers waren auf mehreren LTO-6-Sicherungsbändern gespeichert, die von der Malware gelöscht wurden. In Zusammenarbeit mit der F&E-Abteilung entwickelte Ontrack eine maßgeschneiderte hardware- und softwarebasierte Lösung zur Wiederherstellung von 46 TB Daten auf 18 LTO-6 Sicherungsbändern.

## Über Ontrack

Ontrack, die globale Marke für Datenrettung von KLDISCOVERY, verfügt über 35 Jahre Erfahrung in der Branche, eine Reihe von selbst entwickelten Hardware- und Software-Datenrettungswerkzeugen und ein hochqualifiziertes Team an Datenrettungsingenieuren und Entwicklern. Ontrack bietet erstklassige Datenrettung für alle Arten von Datenverlust und alle Speichermedien: Festplatten, SSDs, Server, NAS, SAN, virtuelle Maschinen, Cloud, Mobilgeräte und Bänder.