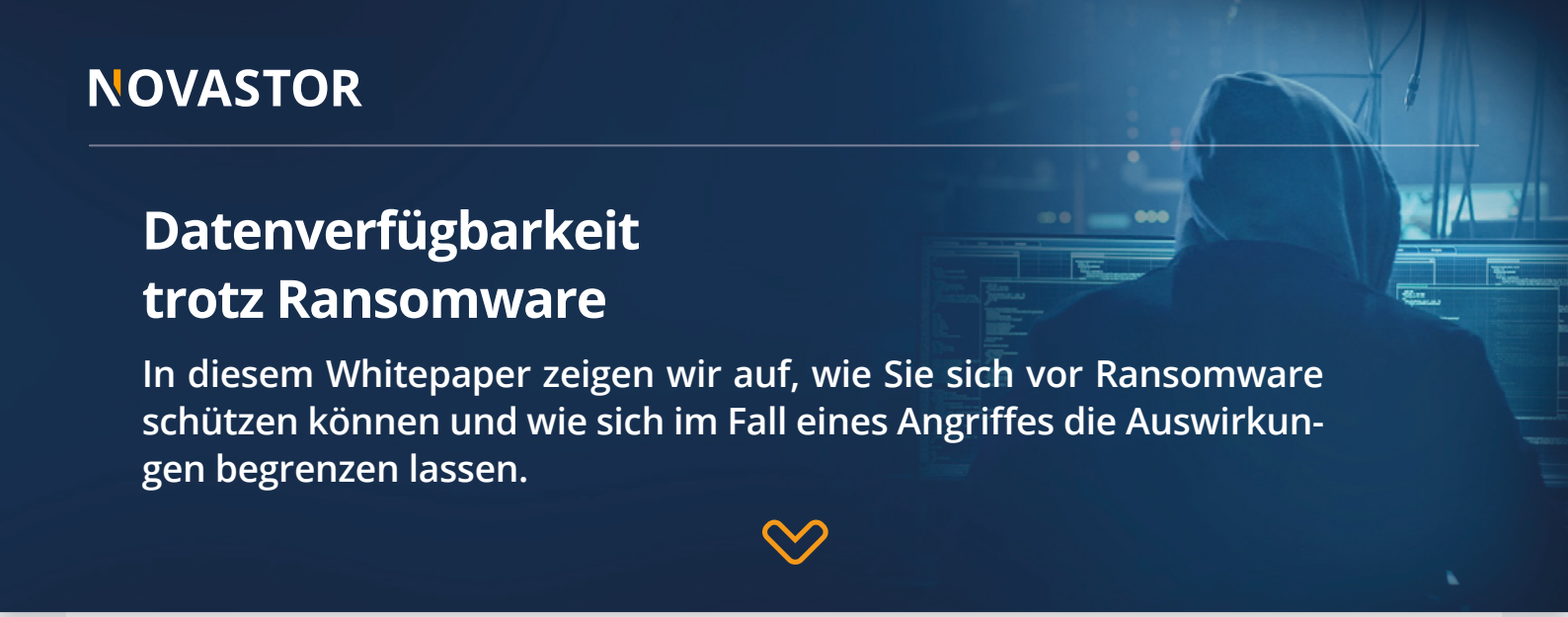
NOVASTOR

Datenverfügbarkeit trotz Ransomware

In diesem Whitepaper zeigen wir auf, wie Sie sich vor Ransomware schützen können und wie sich im Fall eines Angriffes die Auswirkungen begrenzen lassen.



▶ Bedrohungsszenario Ransomware: Unternehmen, Behörden und andere Organisationen sind betroffen.

Die aktuelle Bedrohungssituation

Ransomware hatte es in der Vergangenheit oftmals auf Privatnutzer abgesehen, aber inzwischen sind größere Ziele im Visier der Cyberkriminellen: Behörden und Unternehmen. Prominente Fälle wie die Juwelierkette Wempe haben es auch in Deutschland in die Schlagzeilen geschafft. In den USA gehört unter anderem die Stadtverwaltung von Baltimore zu den Opfern. Laut IT-Security-Spezialist Malwarebytes stieg die Zahl der Ransomware-Angriffe auf Firmen im zweiten Halbjahr 2018 um 88 Prozent.

Zu den wichtigsten Einfallstoren für Schadsoftware gehören veraltete Anwendungen und Betriebssysteme, wie beispielsweise bei der verheerenden „WannaCry"-Attacke aus dem Jahr 2017: Über 220.000 Systeme in mehr als 150 Ländern waren davon betroffen. Mit „BlueKeep" gibt es aktuell eine neue Bedrohung: eine Sicherheitslücke in zahlreichen älteren Windows-Versionen. Experten befürchten, dass auch sie sich, wie im Fall WannaCry, automatisiert ausnutzen lässt.

Zu weiteren bekannten Angriffswegen zählen Phishing-E-Mails, die beispielsweise eine Bewerbung vortäuschen und die Malware als harmlos scheinenden Anhang mitsenden. Die Schadsoftware „GermanWiper" zählt dazu, die besonders unverfroren vorgeht: Sie verlangt ein Lösegeld, obwohl sie die Daten bereits unwiederbringlich überschrieben hat.

Die Liste möglicher Schwachstellen ließe sich fortsetzen: Social Engineering, mit Malware infizierte Werbung oder gefälschte Websites sind einige Beispiele dafür.

Kommt es zu einem erfolgreichen Angriff, sind die Kosten enorm: Sie reichen von stillstehenden Geschäftsprozessen bis hin zu entgangenen Umsätzen oder auch Konventionalstrafen. In der Folge möchten wir Ihnen aufzeigen, wie Sie einem solchen Ernstfall vorbeugen können und wie Sie sich richtig darauf vorbereiten, falls es doch dazu kommt.

Tipps und Schutzmaßnahmen

Um es Ransomware und anderer Schadsoftware schwerer zu machen, sollten verschiedene Grundlagen gegeben sein. Dazu gehört eine aktuelle Antivirus-Software. Sie kann zwar nur bekannte Bedrohungen aussperren, aber das senkt das Gefahrenpotenzial bereits beträchtlich. Eine vorgeschaltete Firewall mit aktiven Filtern ist wichtig. Außerdem sollten Sie die Rechte an den Arbeitsplatz-PCs und im Netzwerk sinnvoll und strikt umsetzen. Das wird manche Handgriffe für die Mitarbeiter eventuell etwas umständlicher machen, dafür erschweren Sie es einer Schadsoftware, tief ins System einzudringen. Vermitteln Sie entsprechend die Wichtigkeit dieser Schutzmaßnahme. Dazu kann es ebenfalls gehören, die USB-Anschlüsse an den Rechnern zu blockieren und Betriebssysteme zu verbannen, die keine Sicherheitsupdates mehr bekommen.

Apropos Betriebssysteme: Laut Security Test zielen sieben von zehn Schadprogrammen auf Windows ab. Wenn Sie einen Backup-Server unter Linux nutzen, wehren Sie schon auf diese Weise eine Reihe von Ransomware-Attacken ab. Verlassen Sie sich allerdings nicht vollständig darauf, denn auch für Linux gibt es entsprechende Schadsoftware.

> **Tipp in eigener Sache:**
> Mit NovaStor DataCenter können Sie sehr einfach Ihren Backup-Server unter Linux betreiben.

Nutzen Sie eine abgekapselte virtuelle Maschine für solche Rechner, die viel mit externen E-Mails arbeiten, z.B. in Abteilungen wie Human Resources.

Isolieren Sie unbekannte Computer im Netzwerk. Schaffen Sie hier zudem klare Regeln für Geräte, die die Mitarbeiter selbst mitbringen.

Nehmen Sie wichtige Daten wie Sicherungen offline. Stichwort: air gap. Ransomware ist heute schlau genug, um sich im lokalen Netzwerk zu verbreiten und dort nach wertvollen Dateien oder Backups zu suchen. Aber nicht alles muss jederzeit zugriffsbereit sein. Nutzen Sie also zum Beispiel Wechselmedien wie Tapes, die sich auswerfen lassen. In einer Tape Library sind alle Datensicherungen automatisch geschützt, wenn sie nicht gerade beschrieben werden.

Auf diese Weise können Sie Daten außerdem sehr gut langfristig aufbewahren. Denn bedenken Sie, dass Ransomware häufig nicht sofort aktiv wird. Die eigentliche Infektion kann bereits Tage oder Wochen zurückliegen. Deshalb brauchen Sie im Fall der Fälle längerfristige Backups.

Vergessen Sie bei alldem nicht die wichtigste potenzielle Sicherheitslücke: die Person vor dem Rechner. Schulen Sie die Mitarbeiter und weisen Sie dabei besonders auf Techniken wie Social Engineering hin. Alle Mitarbeiter müssen außerdem genau wissen, wie sie im Falle eines Angriffs vorgehen sollen.

Ganzheitliche Backup-Strategien als Schutz

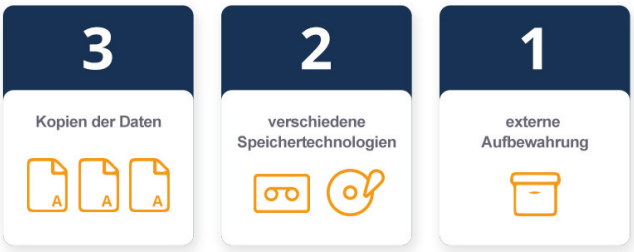
Einen hundertprozentigen Schutz gegen eine Ransomware-Attacke wird es trotz allem nicht geben. Aber mit der richtigen Prävention und der passenden Backup-Strategie können Unternehmen, Behörden und Systemhäuser Ihre Daten für den Fall eines Cyber-Angriffs optimal schützen.

Neben einer leistungsstarken, zuverlässigen Software bedarf es hier einer durchdachten Backup-Strategie: Welche Daten sollen in welchen Abständen wohin gesichert werden? Wie viele Kopien einer Sicherung sind sinnvoll und wo werden diese aufbewahrt?

Die Antworten auf diese Fragen können entscheidend sein, wenn es darum geht, das Überleben des Unternehmens zu sichern.

▶ Eine gute Backup-Strategie kann Ihre Daten vor Ausfällen, u.a. durch Cyber-Angriffe, Feuer oder Wasserschäden schützen.

Außerdem sollte der Backup Server auf einem eigenständigen physischen Server laufen und dabei so weit wie möglich vom produktiven Netzwerk abgeschottet sein. So schützen Sie Ihre Backup-Infrastruktur und Backup-Speicher vor einem Übergriff und können im Notfall sofort die Wiederherstellung starten.



Grundlage: 3-2-1 Backup-Strategie

Obwohl die 3-2-1 Regel selten in Geschäftsvorschriften oder offiziellen Richtlinien zu finden ist, hat sie sich als Standard für Backup-Strategien bewährt und ermöglicht Unternehmen, im Falle eines Angriffs oder anders verursachter Ausfallzeiten den Betrieb rasch wieder aufzunehmen.

Sie sollten insgesamt drei Kopien wichtiger Geschäftsdaten haben, die auf zwei verschiedenen Medientypen gespeichert sind und Sie sollten eine Kopie extern aufbewahren.

Diese Strategie wird nicht zuletzt deshalb noch dringlicher, weil Ransomware selbst nach Lösegeldzahlung die Daten nicht in jedem Fall wiederherstellt. Die weiter oben bereits erwähnte Schadsoftware GermanWiper ist ein dramatisches Beispiel dafür: Sie verschlüsselt die Daten nicht, sondern überschreibt sie.

In solchen Fällen ist ein unbeschädigtes Backup die einzige Möglichkeit, die Geschäftsfähigkeit wiederherzustellen. Mit der 3-2-1 Regel sorgen Sie dafür, dass Ihre Organisation in jedem Fall über ein solches Backup verfügt.

Dieses Vorgehen ist nebenbei bemerkt ebenfalls sinnvoll als Schutz gegen Feuer, Wasserschäden oder im Falle eines Einbruchs.

Tipp in eigener Sache:

Im Rahmen von NovaStors Installationsservice richten wir Ihre Backups ein, führen Sie in die Software-Funktionen ein und setzen ausgewählte Backup-Jobs auf.

Backup-Konzept und IT-Notfallhandbuch

Bei der Datensicherung gibt es also viel zu bedenken. Und hier kommt NovaStor als Lösungsanbieter ins Spiel: Wir übernehmen Verantwortung für die Datensicherung unserer Kunden und helfen unseren Partnern.

Ein hilfreiches, unverzichtbares Duo sind dabei Backup-Konzept und IT-Notfallhandbuch. Während das Backup-Konzept detailliert festhält, wie Ihre Datensicherung aufgebaut ist, sorgt das IT-Notfallhandbuch dafür, dass aus einer schwierigen Situation keine Katastrophe wird.

Das (schriftlich festgehaltene) Backup-Konzept erleichtert beispielsweise den Backup-Nachweis in Unternehmensprüfungen. Es hilft außerdem dabei, die Datensicherung transparent zu machen und neue Kollegen oder Vertretungskräfte einzuarbeiten. Nicht zuletzt ist es die Basis für einen Notfallplan.

> *„Das Backup-Konzept bildet die optimale Backup-Strategie und -Infrastruktur ab, die alle wesentlichen Anforderungen und Bedrohungsszenarien bei möglichst geringen Kosten berücksichtigt.“*

Wolfgang Rudloff
Senior Backup Consultant bei NovaStor

Was findet sich konkret im Backup-Konzept?

Für das Backup-Konzept erfassen NovaStors Experten Ihre IT-Umgebung mit sämtlichen Systemen, Datenmengen und weiteren Eckdaten der unternehmensweiten Datensicherung.

Ihre Anforderungen gleichen wir dabei mit den aktuellen Gegebenheiten ab. So weisen NovaStors Backup-Konzepte beispielsweise Sicherheitslücken aus oder zeigen eine effizientere Speichernutzung auf. Wir empfehlen außerdem Optimierungen und liefern konkrete Lösungsansätze, die Ihre Ziele berücksichtigen.

Im Einzelnen bedeutet das:

1.

Das Backup-Konzept hält den technischen, organisatorischen und gesetzlichen Rahmen fest.

Es versammelt die externen und internen Anforderungen. Dazu gehören alle geschäftskritischen Anwendungen und Prozesse. Außerdem schafft es eine Übersicht dazu, welche Gesetze und Regelungen Sie beachten müssen. Nicht zuletzt finden sich an dieser Stelle Verantwortlichkeiten und Abläufe rund ums Backup.

2.

Es zeigt Bedrohungsszenarien und Gegenmaßnahmen auf.

Dazu gehört natürlich der Schutz vor Ransomware und anderen Cyber-Attacken. Hier listet es folglich auf, welche Maßnahmen dagegen zum Einsatz kommen.

3.

Es hält detailliert fest, wie die Backup-Strategie ausgehend von diesen beiden Punkten aussieht.

Wie werden die Daten geschützt? Was wird wo gespeichert? Wie oft erfolgen welche Sicherungen? Wie sind die verschiedenen Elemente miteinander verbunden?

Das Backup-Konzept lässt sich bei NovaStor DataCenter übrigens in der Software abbilden und ist dann automatisch auf dem neuesten Stand. Gerade für Audits ist das eine große Erleichterung.

Tipp in eigener Sache:

NovaStor unterstützt Sie dabei, Ihre Datensicherungslösung rechtskonform aufzusetzen sowie Backup-Strategien für Eventualitäten, wie z.B. Cyber-Attacken zu optimieren und zu dokumentieren. Von der Erstellung eines Backup-Konzeptes, über die Installation bis hin zur Implementierung der Backup und Restore Software begleiten Sie NovaStors Backup-Experten mit der Erfahrung aus hunderten Datensicherungsprojekten. Sie wählen den Umfang der Service-Leistung, wir sorgen dafür, dass die Datensicherung in Ihrem Unternehmen hundertprozentig zuverlässig läuft.

Das IT-Notfallhandbuch wiederum sorgt dafür, dass im Fall der Fälle klar geregelt ist, was wie getan werden muss und von wem. Sie legen somit Verantwortlichkeiten und Prioritäten fest. Sie geben Handlungsanweisungen und sorgen auf diese Weise dafür, dass wichtige Prozesse und gesetzliche Vorschriften auch im Eifer des Gefechts eingehalten werden.

▶ Versinken Sie nicht im Chaos und halten Sie sich strikt an das Backup-Konzept und IT-Notfallhandbuch.

Implementierung und Backup Health Check

Der beste Plan nützt nichts, wenn er nicht korrekt umgesetzt wird. Hier ist es wichtig, dass Experten Ihre Backup-Lösung fachgerecht implementieren. Sie stellen sicher und zertifizieren, dass der Aufbau den Anforderungen entspricht, so wie im Konzept dargestellt.

Der regelmäßige „Backup Health Check“ wiederum ist unerlässlich, weil Sie sich nicht blind darauf verlassen sollten, dass das Backup und auch der Restore tatsächlich wie gedacht funktionieren. Daher ist eine testweise Wiederherstellung der gespeicherten Daten besonders wichtig.

Ein solcher Funktionstest stellt beispielsweise einzelne Dateien oder auch ganze Verzeichnisse probeweise wieder her. Die Ergebnisse werden in einem Zertifikat festgehalten und dokumentiert.

Leistungsumfang des NovaStor Health Check

- Anruf nach individueller Terminvereinbarung
- Remote Session (Teamviewer) mit einem unserer Backup-Experten
- Überprüfen der Backup- und Restore-Funktionen, Identifikation etwaiger Probleme
- Empfehlung von Optimierungen
- Restore-Test einzelner Dateien oder kleiner Verzeichnisse
- Zeit für individuelle Fragen

Tipp in eigener Sache:

NovaStors Professional Services umfassen verschiedene Leistungen – unsere Backup-Experten erstellen Ihr Backup-Konzept, legen die Backup-Strategie fest, implementieren die Software und führen Restore-Tests für Sie durch. NovaStors Backup und Restore Health Check überprüft die Funktionsfähigkeit Ihrer Datensicherung und dokumentiert die Ergebnisse in einem Zertifikat.

Auf einen Blick: NovaStors Leistungen für Sie

Unsere ganzheitliche Datensicherungslösung visualisiert komplexe Backup-Prozesse übersichtlich, entlastet Backup-Verantwortliche und sorgt dafür, dass Sie das Schlimmste verhindern können, wenn Ihre Organisation von Ransomware angegriffen wird.

NovaStors Komplettlösung umfasst unter anderem eine performante Software, ein Backup-Konzept und regelmäßige Backup Health Checks.

1. Experten entwickeln für Sie ein Backup-Konzept und halten es schriftlich fest.
2. Im nächsten Schritt stellen sie sicher, dass die Sicherung wie gewünscht erfolgen.
3. Und sie testen bereits vorhandene Sicherungen daraufhin, ob die Medien lesbar sind und sich die fraglichen Systeme im gewünschten Umfang wiederherstellen lassen.

Fazit

Ransomware ist ein reales Bedrohungsszenario, über das sich jeder in Ihrer Organisation bewusst sein sollte. Selbst umfassende Schutzmaßnahmen geben Ihnen allerdings keine hundertprozentige Garantie, dass nicht doch ein Einfallstor gefunden wird. Dafür sind die Systeme im Unternehmen und Behörden schlicht zu komplex und zu viele Personen involviert.

Eine umfassende Backup-Strategie ist Ihre Versicherung gegen den Fall der Fälle. Dadurch minimieren Sie die Ausfallzeit und damit einhergehende Verluste. Sie sparen sich das Lösegeld der Erpresser und bewahren den guten Ruf Ihrer Organisation.

Über NovaStor

Als deutscher Hersteller und Lösungsanbieter entwickelt NovaStor Backup und Restore Software und entlastet IT-Abteilungen mit Dienstleistungen von der initialen Konzeption bis in den laufenden Betrieb.

Mit bewährten Datensicherungs- und Archivierungslösungen schützt NovaStor heterogene IT-Infrastrukturen sowie verteilte und wachsende Daten auf sämtlichen Speichertechnologien von Disk über Tape bis Cloud.

NovaStor verbindet Expertise aus hunderten Backup-Projekten mit interner Entwicklungskompetenz, um sowohl Standard- als auch Individualprojekte umzusetzen. Unternehmen, Behörden und Rechenzentren erhalten von NovaStor zukunftssichere Lösungen für Datensicherung und Archivierung.

NovaStor ist inhabergeführt und an drei Standorten vertreten: in Deutschland (Hamburg), den USA (Agoura Hills) und der Schweiz (Rotkreuz).