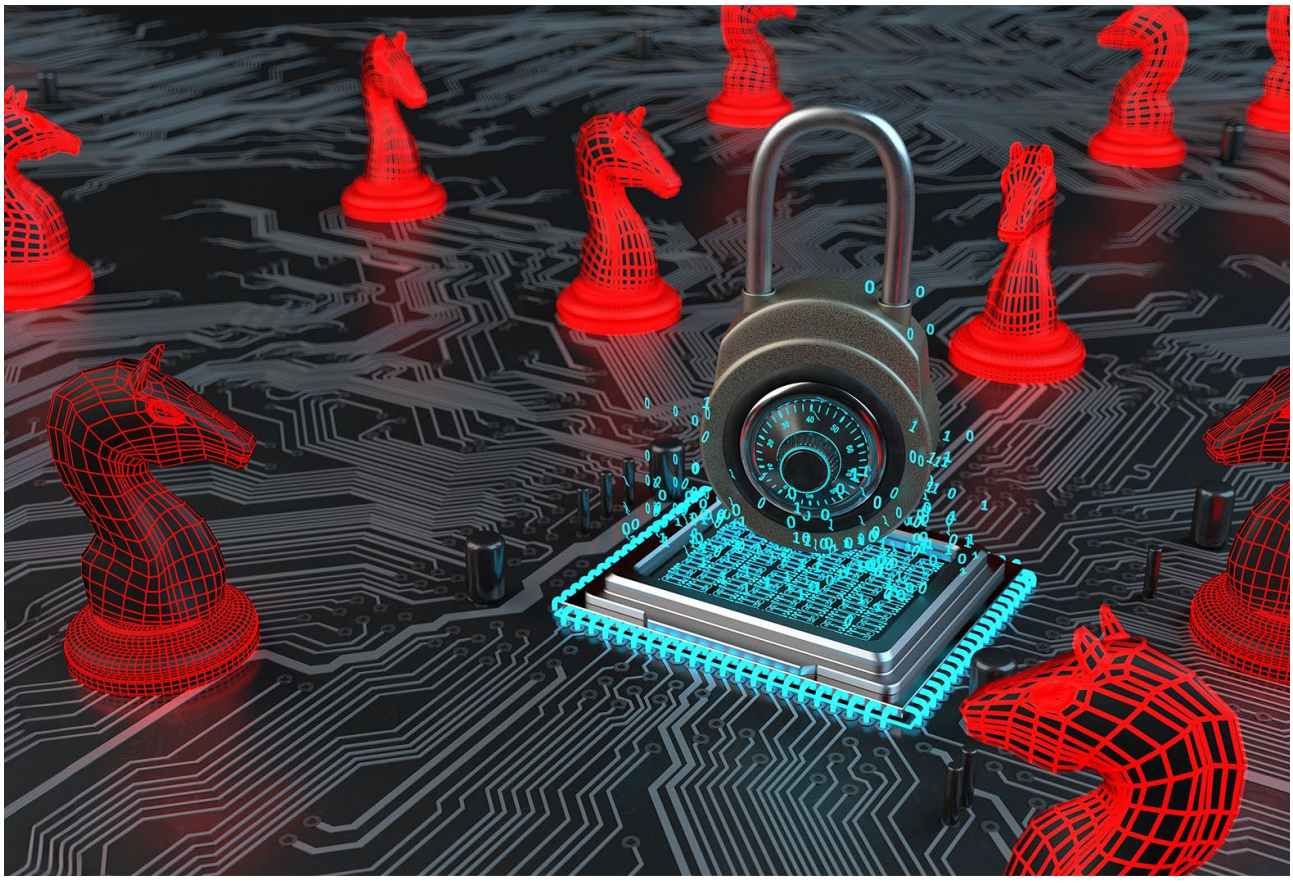
onoff ENGINEERING

Mittelstand-Digital Zentrum Hannover

Best Practice
zu Verschlüsselungstrojaner-resilienten Datensicherungen



Quelle: Alexander Limbach/stock.adobe.com

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Ausführliche Schreibweise
APR	Arbeitsplatzrechner
BSI	Bundesamt für Sicherheit in der Informationstechnik
DSGVO	Datenschutz-Grundverordnung
EU	Europäische Union
KMU	Kleine und mittlere Unternehmen
NAS	Network Attached Storage
RPO	Recovery Point Objective
RTO	Recovery Time Objective
VM	Virtuelle Maschine
VPN	Virtual Private Network
WORM	Write once, read many

Autoren

Jan-Niklas Puls
arbeitet als wissenschaftlicher Mitarbeiter an der Hochschule Hannover und ist Experte für IT-Sicherheit im Mittelstand-Digital Zentrum Hannover.

Prof. Dr.-Ing. Karl-Heinz Niemann
ist Professor für das Fachgebiet Prozessinformatik und Automatisierungstechnik (PIA) an der Hochschule Hannover.

Sebastian Meyer
arbeitet als Ingenieur für die Gebäudeautomation mbH in Hameln, nachdem er das Studium Elektro- und Informationstechnik an der Hochschule Hannover als Bachelor of Engineering abgeschlossen hat.

Haftungsausschluss

Die diesem Dokument zu Grunde liegenden Informationen wurden mit größtmöglicher Sorgfalt recherchiert und zusammengestellt. Dennoch wird dieses ohne eine Gewährleistung zur Verfügung gestellt. Der Autor lehnt ausdrücklich jede Art von vertraglicher oder gesetzlicher Haftung für dieses Dokument ab.

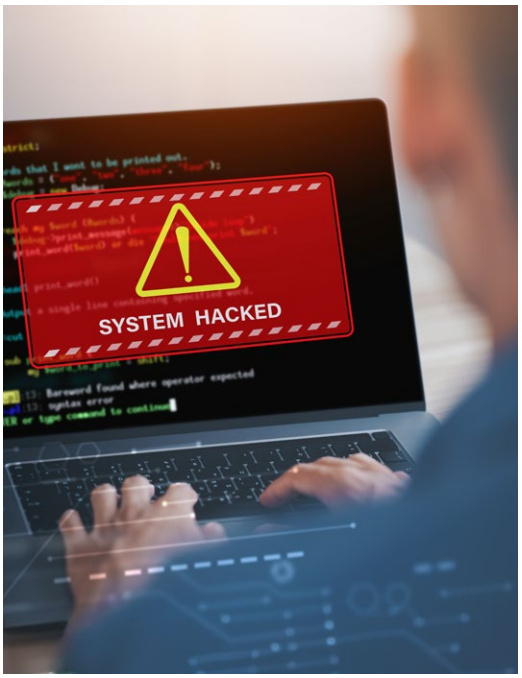
In keinem Fall ist der Autor für Schäden verantwortlich, die durch Fehler oder fehlende Informationen in diesem Dokument entstehen könnten. Logos und Markennamen werden ohne Hinweis auf ggf. bestehende Schutzrechte verwendet.

Version 1.0
Dieses Dokument beschreibt ein Best Practice für Verschlüsselungstrojaner-resiliente Datensicherungen und ist mit Unterstützung von Herrn Sebastian Meyer entstanden, der das Thema im Rahmen seiner Abschlussarbeit vertiefend bearbeitet hat. Ein großer Dank an Herr Meyer sowie die onoff engineering GmbH für die vertrauensvolle und professionelle Zusammenarbeit.

DOI folgt

1 Einleitung

Viele deutsche Unternehmen sind in der Vergangenheit Opfer von Cyberangriffen geworden. Dabei sind große Unternehmen ebenso betroffen wie kleine und mittlere Unternehmen (KMU) [BIT2022]. Der Umgang mit Cybervorfällen variiert von Unternehmen zu Unternehmen. Während große Unternehmen häufig über eigene Strukturen verfügen, die bei der Reaktion auf Cybervorfälle unterstützen, müssen KMU häufig auf externe Expertise zurückgreifen, da keine internen Strukturen vorhanden sind. Im Falle eines Angriffs mit Hilfe eines Verschlüsselungstrojaners ist es essentiell, dass Unternehmen über vollständige und aktuelle Datensicherungen verfügen.



Quelle: Deemerwha studio/stock.adobe.com

Nur mit Hilfe von Datensicherungen ist es möglich, dass Unternehmen nach einem erfolgreichen Angriff durch einen Verschlüsselungstrojaner ihre IT-Systeme schnell wiederherstellen und auf ihre Daten zugreifen können, um anschließend in den Regelbetrieb zurückkehren zu können. Viele Unternehmen, gerade KMU, verfügen allerdings über einen unzureichenden Schutz gegenüber einem Verschlüsselungstrojaner. Zwar sind in den meisten KMU Datensicherungen vorhanden, allerdings suchen moderne Verschlüsselungstrojaner im Unternehmensnetzwerk zunächst aktiv nach bestehenden Datensicherungen und verschlüsseln diese, bevor im Anschluss die Aktivdaten der Mitarbeitenden verschlüsselt werden [BSI2022d]. Häufig wird der Verschlüsselungstrojaner hierbei durch Mitarbeitende - in der Regel ungewollt - in die IT eingebracht und mit Hilfe eines Fernzugriffs durch die Angreifenden gesteuert. Aus diesen Gründen ist es wichtig, dass Unternehmen über Verschlüsselungstrojaner-resiliente Datensicherungen verfügen.

Im Rahmen dieses Best-Practice-Dokuments wird beschrieben, wie ein Datensicherungskonzept für KMU aussehen kann. Hierzu wird zunächst beschrieben was ein Verschlüsselungstrojaner ist und wie dieser vorgeht. Anschließend werden verschiedene Arten von Datensicherungen sowie mögliche Richtlinien und Leitfäden beschrieben. Weiterhin werden technische und organisatorische Voraussetzungen sowie Anforderungen an Verschlüsselungstrojaner-resilienten Datensicherungen dargestellt. Abschließend folgt die Beschreibung eines Best-Practice-Vorgehens für Verschlüsselungstrojaner-resilienten Datensicherungen.

Dieses Dokument ist im Rahmen eines Digitalisierungsprojektes, das in Kooperation mit der onoff engineering GmbH durchgeführt wurde, entstanden. Wir bedanken uns bei der onoff engineering GmbH sowie Herrn Sebastian Meyer für die vertrauensvolle und professionelle Zusammenarbeit.

2 Was sind Verschlüsselungstrojaner?

Bei einem Verschlüsselungstrojaner (engl. Ransomware) handelt es sich allgemein um eine Schadsoftware. Der Begriff kommt ursprünglich aus dem Englischen und setzt sich aus den zwei Komponenten „Ransom" (dt. Lösegeld) und „Software" zusammen. Dabei handelt es sich um eine Schadsoftware, mit der Angreifende darauf abzielen, Daten und Systeme zu verschlüsseln und somit den Zugriff auf diese zu verhindern. Auf den Systemen des Opfers hinterlässt die Software anschließend eine Erpressernachricht mit einer Lösegeldforderung und der Drohung, das zum Entschlüsseln der Daten benötigte Schlüsselmaterial zu vernichten, wenn der Lösegeldforderung nicht nachgegangen werden sollte. Die Höhe des Lösegelds wird häufig erst in direkten Verhandlungen mit den Angreifenden festgelegt. Dabei orientiert sich die Forderung am Gesamtumsatz des Unternehmens [BSI2022b].

Neben der Forderung nach Lösegeld besteht eine weitere Strategie bei Angriffen mit Verschlüsselungstrojanern darin, die Daten vor der Verschlüsselung zu entwenden und zusätzlich mit der Veröffentlichung dieser Daten zu drohen. Dieser Ansatz wird als „Double Extortion" (dt. doppelte Erpressung) bezeichnet, da hierbei neben der Verfügbarkeit der Daten auch deren Vertraulichkeit kompromittiert wird. Sind die Daten vertraulich zu behandeln, wie beispielsweise personenbezogene Daten, ist bereits der Einblick in diese durch unbefugte Personen, wie es Angreifende sind, als Datenschutzvorfall zu werten und im Kontext der Datenschutz-Grundverordnung (DSGVO) zu melden. [EPR2016].

Die Erpressungsmethoden der Angreifenden entwickeln sich immer weiter. So kann es darüber hinaus auch dazu kommen, dass die Angreifenden die gestohlenen Daten nicht nur veröffentlichen, sondern gezielt Kontakt mit Kundeninnen und Kunden des Opfers oder auch mit der Presse oder Aufsichtsbehörden aufnehmen. Diese mehrfache Erpressung führt dazu, dass der Druck auf die Opfer stark zunimmt, sodass diese möglicherweise eher dazu bereit sind, das geforderte Lösegeld zu bezahlen [MS2022].

Die Motivation von Angreifenden zur Verübung von Ransomware-Angriffen ist in den meisten Fällen rein finanziell. Das BSI rät allerdings trotz des erwähnten hohen Drucks beim Opfer grundsätzlich davon ab, den Lösegeldforderungen nachzugehen. Ein Grund dafür besteht darin, dass die Angreifenden durch eine erhaltene Zahlung in ihrem Tun bestärkt werden und in Zukunft weitere Angriffe durchführen sowie höhere Lösegelder fordern. Zudem besteht keine Garantie, dass die Daten nach der Lösegeldzahlung tatsächlich wieder entschlüsselt werden. Häufig werden Unternehmen, die gezahlt haben, nach einiger Zeit auch ein zweites oder drittes Mal angegriffen, um weiteres Lösegeld zu erpressen [BSI2022c].

In der folgenden Tabelle 1 werden die vom BSI am häufigsten verwendeten Angriffsvektoren von Verschlüsselungstrojanern beschrieben, mit denen ein initialer Zugang in Unternehmensstrukturen gelingt.

Angriffsvektor	Erklärung
SPAM	Meist soll das potenzielle Opfer hierbei durch professionelles Social Engineering zum Öffnen von E-Mail-Anhängen bewegt werden. Die Schadsoftware wird dann per Download nachgeladen oder ist bereits als ausführbare Datei im Anhang enthalten. Betrifft insbesondere PDF-, Word- und Excel-Dateien.
Drive-By-Infektionen mittels Exploit-Kits	Schwachstellen in weit verbreiteten Programmen werden in Exploit-Kits integriert, die Verbreitung erfolgt meist über kompromittierte Webseiten oder Werbebanner mit nachgeladener Ransomware.
Serverschwachstellen	Eindringen der Angreifenden in einen vom potenziellen Opfer bereitgestellten Webserver durch die Ausnutzung von Schwachstellen oder das Erraten schwacher Passwörter.
Ungeschützte Fernzugänge	Scannen des Internets nach Systemen mit Fernzugängen mit anschließenden Brute-Force-Angriffen auf Passwörter.

Tabelle 1: Die am meisten verwendeten Angriffsvektoren von Verschlüsselungstrojanern, angelehnt an [BSI2022c]

Abbildung 1 zeigt, wie ein beispielhafter Ransomware-Angriff ablaufen könnte. Als Basis dient in diesem Beispiel die erfolgreiche Infektion eines Rechners durch eine Spam-Mail, bei der das Opfer den Anhang, beispielsweise eine Word oder PDF-Datei, geöffnet hat. Anschließend versucht der Angreifende, sich möglichst weit lateral im Unternehmensnetzwerk auszubreiten. Dies kann auch manuell, z. B. mit Hilfe eines Fernzugriffs erfolgen. Vor der Verschlüsselung erfolgt hierbei, wie bereits oben beschrieben, das Stehlen der Daten, welche ggf. auf einer vom Angreifenden betriebenen Leak-Webseite veröffentlicht werden. Nach der Verschlüsselung durch den nachgeladenen und im Netzwerk verbreiteten Verschlüsselungstrojaner wird das Opfer durch eine Erpressernachricht zur Zahlung über ein Bezahlportal aufgefordert. Die Zahlung erfolgt dabei aus Anonymitätsgründen häufig in Form von Kryptowährungen wie zum Beispiel Bitcoin oder Monero [BSI2022b], [BSI2022c].

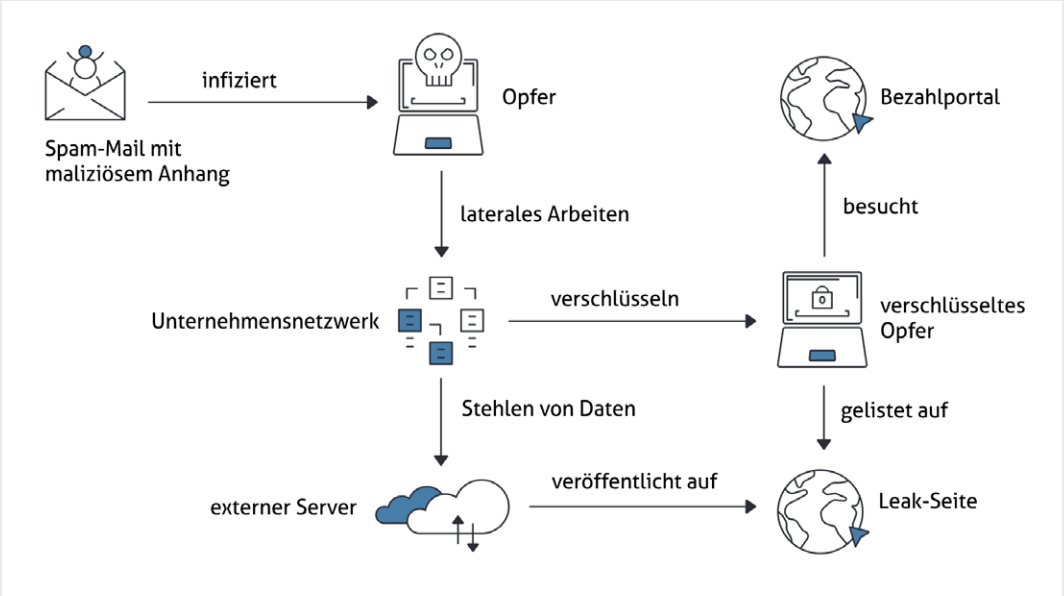


Abbildung 1: Beispielhafter Ablauf eines Angriffs durch einen Verschlüsselungstrojaner [BSI2022b]

Das beschriebene Angriffsmuster macht klar, dass nach einem Angriff zwei mögliche Szenarien betrachtet werden können:

1. Das Verhindern der Veröffentlichung von Unternehmensdaten durch die Lösegeldzahlung (nicht empfohlen).
2. Die Wiederherstellung der verschlüsselten Daten durch
    a. Lösegeldzahlung (nicht empfohlen) oder durch
    b. Bereinigung der Systeme und Rückspielen einer Datensicherung (Backup).

Dieses Dokument befasst sich im Weiteren mit der Variante 2b und hier insbesondere mit der Erstellung und dem Rückspielen der Datensicherung.

3 Arten von Datensicherungen

In diesem Kapitel werden zwei verschiedene Datensicherungsarten beschrieben. Hierbei wird zwischen Volldatensicherung und der inkrementellen Sicherung unterschieden. Außerdem wird die 3-2-1 Regel beschrieben und erklärt.

3.1 Volldatensicherungen

Bei der Volldatensicherung wird der Gesamtbestand der zu sichernden Daten zu jedem Sicherungszeitpunkt vollständig gesichert. Es ist dabei unerheblich, ob sich die Daten im Gegensatz zur vorherigen Sicherung geändert haben oder nicht. Aus diesem Vorgehen ergibt sich der Nachteil, dass eine Volldatensicherung, im Vergleich zu anderen Sicherungsverfahren, viel Speicherplatz benötigt (siehe Abbildung 2).

Ein Vorteil dieses Vorgehens besteht darin, dass im Falle der Wiederherstellung alle Daten auf Basis von nur einer Volldatensicherung wiederhergestellt werden können, was den Wiederherstellungsprozess beschleunigt und vereinfacht [BSI2022a].

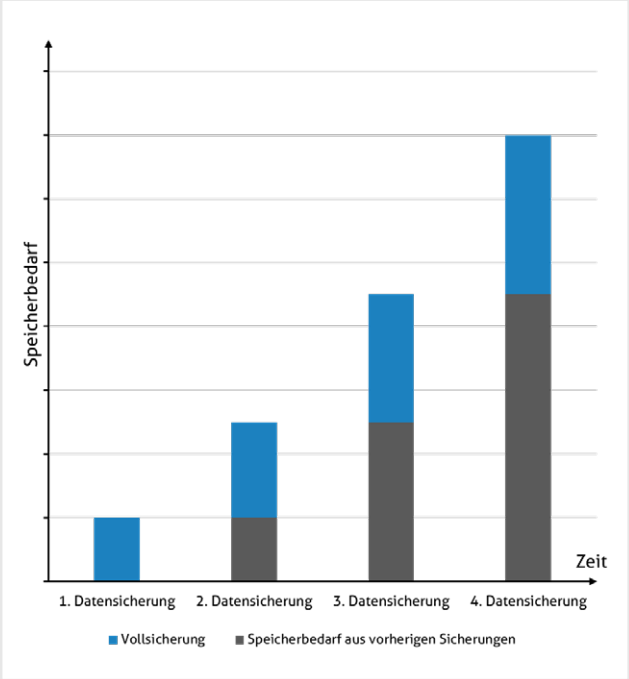


Abbildung 2: Speicherbedarf über die Zeit einer Volldatensicherung

3.2 Inkrementelle Datensicherung

Inkrementelle Datensicherungen haben eine Volldatensicherung als Grundlage. Bei den nachfolgenden Sicherungen werden danach nur jene Daten gesichert, welche sich seit der letzten Sicherung geändert haben. Dabei spielt es keine Rolle, ob die vorherige Sicherung eine Volldatensicherung oder eine inkrementelle Sicherung ist.

Abbildung 3 zeigt, dass bei den der Volldatensicherung nachfolgenden inkrementellen Sicherungen nur die hellgrau markierten Bereiche als zusätzlicher Speicherbedarf benötigt werden, während die dunkelgrau markierten Bereiche den Speicherbedarf aus bereits durchgeführten Sicherungen darstellen. Auf diese Weise entsteht der Vorteil, dass diese Art der Datensicherung bedeutend weniger Speicherplatz benötigt als eine Vollsicherung und somit auch die Dauer des Sicherungsprozesses verkürzt wird. Der Nachteil entsteht jedoch darin, dass der Wiederherstellungsprozess erschwert wird, da zunächst die letzte Volldatensicherung wiederhergestellt werden muss und anschließend die darauf basierenden inkrementellen Sicherungen [BSI2022a].

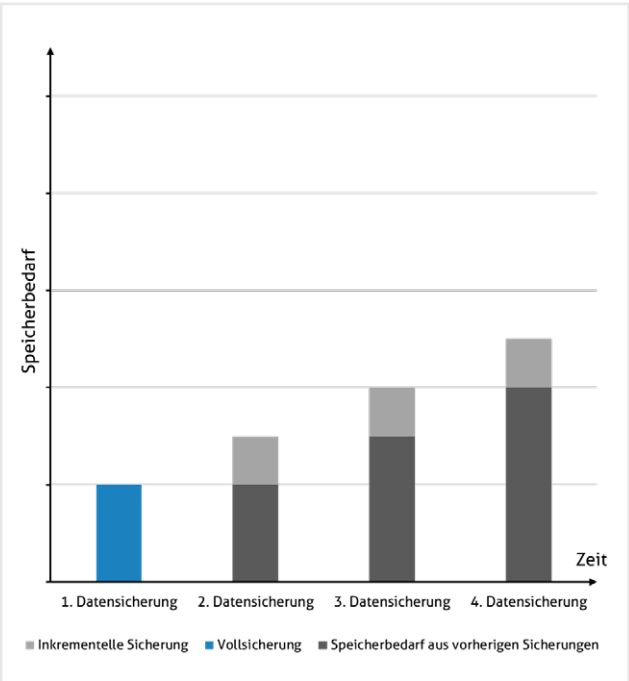


Abbildung 3: Speicherbedarf über die Zeit einer Volldatensicherung

3.3 Häufigkeit und Zeitpunkt zur Durchführung von Datensicherungen

Bei der Festlegung der Häufigkeit der Datensicherungen ist die Frage zu stellen, wie viele Daten zwischen der letzten verfügbaren Datensicherung und einem möglichen Ausfall des Betriebs maximal verloren gehen dürfen. Diese Kenngröße wird auch als Recovery Point Objective (RPO) bezeichnet und wird in Abbildung 4 dargestellt.

Einen entscheidenden Einfluss auf die Wahl der Sicherungshäufigkeit hat das Änderungsvolumen der Daten. Im Falle eines hohen Änderungsvolumens oder einer hohen Verfügbarkeitsanforderung ist es sinnvoll, das Zeitintervall zwischen zwei Sicherungen nicht zu groß zu wählen, um einen möglichen Datenverlust zu minimieren.

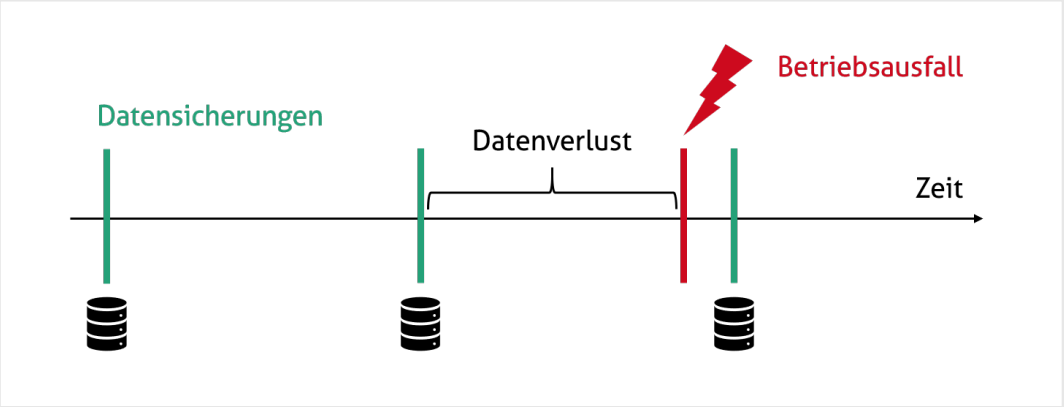


Abbildung 4: Veranschaulichung Recovery Point Objective

3.4 Die 3-2-1 Regel für Datensicherungen

Neben der Festlegung der Datensicherungsart ist es ebenfalls wichtig, dass genügend Datensicherungen vorhanden sind. Dies ist elementar, da Datensicherungslösungen eine begrenzte physische Lebensdauer haben, durch Verschlüsselungstrojaner kompromittiert werden oder einer physischen Gefahr, beispielsweise Feuer, zum Opfer fallen können. Um diesen Gefährdungen entgegenzutreten bietet es sich an, die 3-2-1-Regel im Unternehmen umzusetzen. Die drei Ziffern der Regel stehen konkret für folgende Punkte [NIST2020]:

- Die **3** steht für drei vorhandene Datensätze, wodurch neben den Aktivdaten, mit denen täglich gearbeitet wird, mindestens zwei weitere Datensicherungen vorhanden sein müssen.
- Die **2** steht für **zwei verschiedene Speichermedien**, auf denen die Daten zu sichern sind. Hierbei können beispielsweise zwei verschiedene Festplatten unterschiedlichen Typs verwendet werden. Alternativ ist eine Datensicherung beispielsweise auf Festplatten zu sichern und eine weitere auf Magnetbändern. Die verschiedenen Speichermedien werden im Kapitel 4.3 Auswahl von passenden Speichermedien dargestellt.
- Die **1** steht für die Lagerung der Datensicherungen **an einem anderen Ort**. Hierbei kann es sich beispielsweise um einen anderen Unternehmensstandort oder einen anderen Brandabschnitt handeln. Das bedeutet, dass sich Server und Datensicherung nicht im selben Raum befinden, da im Falle eines Brandes beide Speichermedien physisch zerstört werden.

4 Technische und organisatorische Voraussetzungen für Datensicherungen

Dieses Kapitel beschreibt allgemeine Einflussfaktoren, die auf ein Datensicherungskonzept einwirken können sowie spezifische organisatorische und technische Voraussetzungen, wie die Anzahl der zu verwendenden Datensicherungsgenerationen, die passende Auswahl von zu nutzenden Speichermedien, den Aufbewahrungsort dieser sowie personelle Zuständigkeiten sowie spezifische Richtlinien.

4.1 Einflussfaktoren

Bei der Planung eines Datensicherungskonzeptes gilt es einige Faktoren zu berücksichtigen, welche einen direkten Einfluss auf die Verfahrensweise und die Umsetzung der Datensicherungen haben. Diese Einflussfaktoren müssen für jedes zu sichernde IT-System definiert werden. Dies geschieht in direkter Absprache mit den entsprechenden Verantwortlichen der IT-Systeme. Ein IT-System kann hierbei beispielsweise ein Server sein, auf dem Unternehmensdaten zentral gespeichert sind. Es kann sich aber auch um einen einzelnen Client im Unternehmensnetzwerk handeln. Im Folgenden sind die wichtigsten zu definierenden Einflussfaktoren, die sich an [BSI2023a] und [BSI2022a] orientieren, für Datensicherungen beschrieben.

Spezifikation der zu sichernden Daten
Es sollte festgelegt werden, welche spezifischen Daten des IT-Systems gesichert werden sollen. Dies umfasst alle Daten, welche zur Neueinrichtung des Systems benötigt werden. Zu berücksichtigen sind hierbei Anwendungssoftware, Systemdaten wie zum Beispiel Passwortdateien oder Konfigurationsdaten, Anwendungsdaten sowie Protokolldaten. Weiterhin sind unter anderem Daten zu sichern, die im Zuge von Gesetzen oder Verpflichtungen gegenüber Kundinnen und Kunden vorgehalten werden müssen sowie für das Unternehmen wichtige, selbst erstellte Dokumente und Dateien. Das Betriebssystem selber ist nicht Teil der Sicherungen.

Verfügbarkeitsanforderungen
Verfügbarkeit beschreibt die Eigenschaft, zugänglich und nutzbar zu sein, wenn eine befugte Entität Bedarf hat [DIN_EN_ISO_27000]. Eine geeignete Methode zur Bestimmung der Verfügbarkeitsanforderungen der zu sichernden Daten besteht darin, die maximal tolerierbare Ausfallzeit dieser Daten festzulegen (siehe 3.3 Häufigkeit und Zeitpunkt zur Durchführung von Datensicherungen).

Vertraulichkeitsanforderungen
Vertraulichkeit beschreibt die Eigenschaft, dass Informationen unbefugten Personen, Entitäten oder Prozessen nicht verfügbar gemacht oder offengelegt werden [DIN_EN_ISO_27000]. Hierbei gilt es zu beachten, dass die Vertraulichkeit der Daten ebenso für die erstellten Datensicherungen gilt.

Integritätsanforderungen
Integrität beschreibt die Eigenschaft der Richtigkeit und Vollständigkeit [DIN_EN_ISO_27000]. Datensicherungen dürfen während der Aufbewahrung nicht verändert werden. Bei hohen Integritätsanforderungen der zu sichernden Daten ist bei der Datensicherung ein besonderes Augenmerk darauf zu legen.

Speichervolumen
Der Bedarf an Speicherplatz für die Gesamtheit der zu sichernden Daten.

Änderungsvolumen
Die Gesamtheit der Daten, welche sich in einem bestimmten Zeitraum ändern. Hierbei ist zu unterscheiden zwischen Daten, welche sich inhaltlich ändern und Daten, welche in diesem Zeitraum neu erstellt werden.

Änderungszeitpunkte
Es sollte bestimmt werden, zu welchen Zeitpunkten sich die Daten jeweils ändern. Es kann vorkommen, dass sich bestimmte Daten immer zu den gleichen Zeitpunkten ändern, sodass diese auch immer an diesen Zeitpunkten gesichert werden sollten.

Rechtliche Anforderungen
Bei den zu sichernden Daten muss geprüft werden, ob Fristen, beispielsweise Gesetze, bestehen, welche eingehalten werden müssen. Dies können Aufbewahrungsfristen sein, welche festlegen, wie lange die Daten mindestens aufbewahrt werden müssen oder auch Löschfristen, welche ein Löschen der Daten nach einer bestimmten Zeit erfordern.

Rekonstruktionsaufwand ohne Datensicherung
Es ist festzustellen, ob und mit welchem Aufwand es möglich ist, verlorengegangene Daten zu rekonstruieren, wenn von diesen Daten keine Datensicherung existiert. Bei diesem Punkt geht es um Wirtschaftlichkeit, da jede zu sichernde Datei den Speicherbedarf und damit die Kosten der Datensicherung erhöht.

4.2 Anzahl Datensicherungsgenerationen

Neben der Umsetzung der 3-2-1-Regel (siehe Kapitel 3.4 Die 3-2-1 Regel für Datensicherungen) ist es wichtig, dass ebenfalls verschiedene Generationen von Datensicherungen im Unternehmen vorhanden sind. Bei Generationen handelt es sich um verschiedene Volldatensicherungen, die jeweils unterschiedlich alt sind. So gibt es Datensicherungen von heute und welche die einen Monat, ein halbes Jahr oder ein Jahr alt sein können.

Hintergrund für die Umsetzung von verschiedenen Datensicherungsgenerationen ist es, dass ein Verschlüsselungstrojaner bereits länger inaktiv im Unternehmen sein kann. Grund hierfür kann sein, das Angreifende häufig nicht nur ein Unternehmen angreifen, sondern mehrere gleichzeitig. Dies führt dazu, das Angreifende über einen großen Backlog verfügen. Das bedeutet, dass noch eine große Menge an nicht abgeschlossenen Arbeiten vorhanden sind, die zunächst abgearbeitet werden, bevor der inaktive Verschlüsselungstrojaner aktiviert wird. Der inaktive Verschlüsselungstrojaner wird in diesem Szenario mit in den Datensicherungen gesichert. Um den Verschlüsselungstrojaner mit Gewissheit entfernen zu können, wird nun eine Datensicherung benötigt, die vor der Infiltration des Verschlüsselungstrojaners durchgeführt wurde.

Wenn beim Auftreten einer der beschriebenen Möglichkeiten keine passende Generation mehr vorhanden ist, tritt trotz Datensicherung ein Datenverlust auf. Um dies möglichst zu verhindern, gilt es festzulegen, wie hoch das Mindestalter der ältesten aufzubewahrenden Generation sein soll. Hierbei sind ebenfalls die Einflussfaktoren aus Kapitel 4.1 Einflussfaktoren mit zu berücksichtigen. Je höher das Mindestalter dabei ist, desto größer ist die Wahrscheinlichkeit, dass verlorengegangene Daten oder Daten mit Integritätsverlust auch nach längerer Zeit wiederhergestellt werden können. Dabei muss allerdings auch ein Kompromiss in Bezug auf die Wirtschaftlichkeit getroffen werden, denn mehr aufbewahrte Generationen bedeuten höhere Kosten. Zusätzlich muss in Betracht gezogen werden, dass je älter die zu verwendende Datensicherung ist, desto weniger aktuelle Daten sind vorhanden. Beispielsweise ist die zu verwendende Datensicherung sechs Monate alt, dann fehlen ebenfalls die neu generierten Daten der letzten sechs Monate [BSI2023a].

Eine häufig genutzte Methode zum Aufbewahren von Generationen stellt außerdem das sogenannte Drei-Generationen-Prinzip dar, bei dem ein Rotationsschema mit täglichen, wöchentlichen und monatlichen Sicherungen stattfindet. Dabei könnten die täglichen Sicherungen inkrementell realisiert werden und am Ende einer Woche zu einer wöchentlichen Vollsicherung zusammengefasst werden. In der nächsten Woche werden die täglichen Sicherungen dann mit den neuen Sicherungen überschrieben. Am Ende des Monats wird eine Monatssicherung erstellt.

Die wöchentlichen Sicherungen werden schließlich ab dem zweiten Monat ebenfalls durch die neuen Wochensicherungen überschrieben. Die monatlichen Sicherungen können je nach Bedarf aufbewahrt werden. Bei zum Beispiel zwölf aufbewahrten Monatssicherungen lassen sich die ältesten gesicherten Daten ein Jahr lang wiederherstellen. In Abbildung 5 auf der folgenden Seite ist das Drei-Generationen-Prinzip zur besseren Verständlichkeit anschaulich am Beispiel eines zehn Wochen dauernden Zeitraums dargestellt.

Die Bezeichnungen S1-S4 stehen dabei für die täglichen, V1-V4 für die wöchentlichen und G1-G2 für die monatlichen Sicherungen. Die täglichen Sicherungen sind in Blau, die Wöchentlichen in Grün die monatlichen in Rot dargestellt [BRE2022].

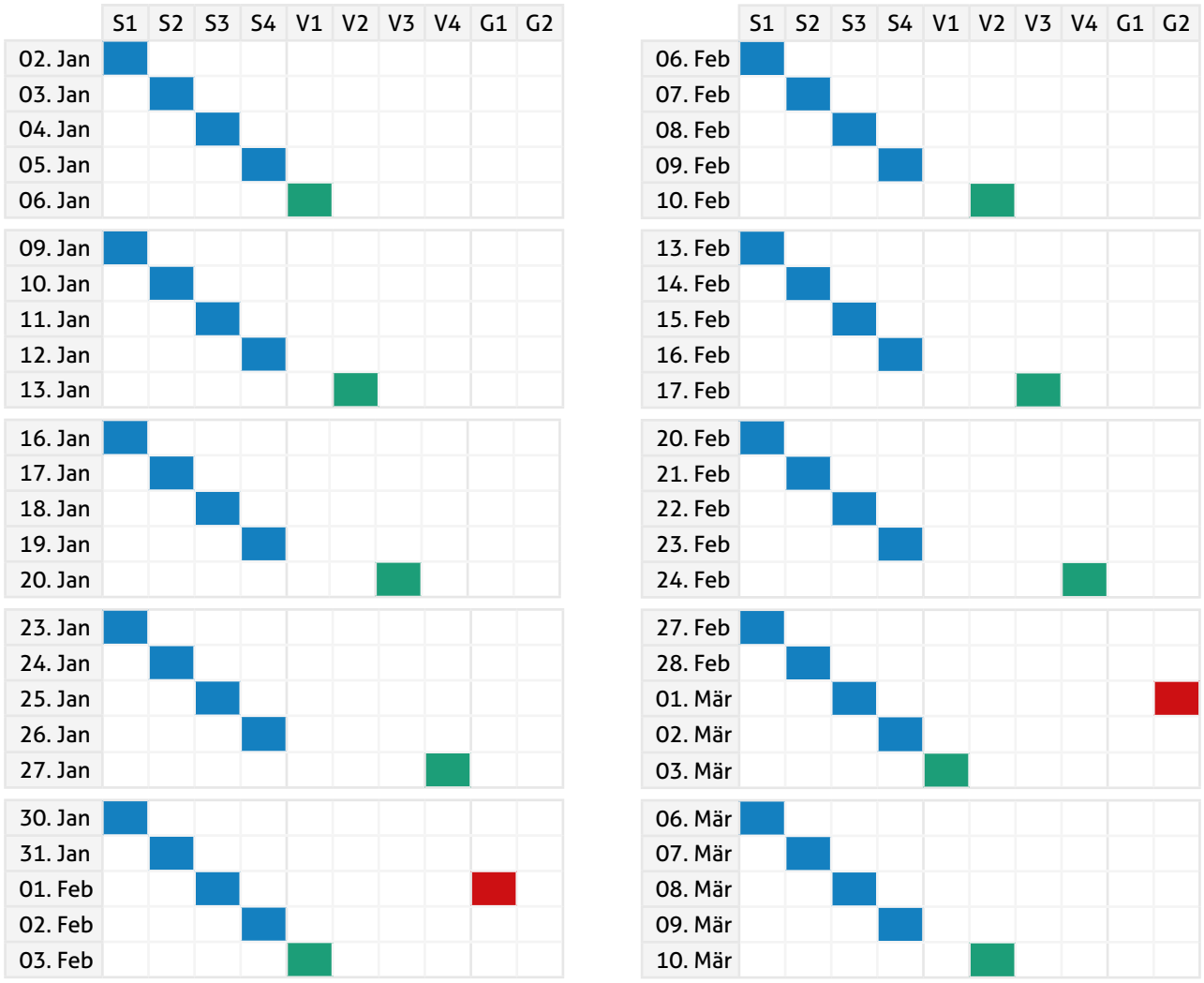


Abbildung 5: Beispielhaftes Drei-Generationen-Prinzip

4.3 Auswahl von passenden Speichermedien

Neben der Umsetzung von verschiedenen Datengenerationen sowie der Nutzung der 3-2-1 Regel ist ebenfalls die Wahl von passenden Speichermedien zu berücksichtigen.

In Tabelle 3 auf der folgenden Seite sind verschiedene Speichermedien mit den jeweiligen Vor- und Nachteilen aufgelistet. Betrachtet werden hierbei Storage-Systeme (z. B. Netzwerkspeicher), mobile Wechseldatenträger (z. B. externe Festplatten), optische Datenträger (z. B. CD, DVD, Blu-ray), Bandlaufwerke sowie die Cloud als Datenspeicher.

	Vorteile	Nachteile
Optische Datenträger	• geringe Anschaffungskosten • Trennung vom Netzwerk nach dem Speichern der Daten	• geringe Speicherkapazität • Die Laufwerke sind empfindlich gegenüber Erschütterungen, Stürzen usw. • ggf. geringe Lebensdauer je nach Medium
Mobile Wechseldatenträger	• geringe Anschaffungskosten • Trennung vom Netzwerk nach dem Speichern der Daten • einfache Bedienung • höhere Speicherkapazität als optische Datenträger	• empfindlich gegenüber Erschütterungen, Stürzen, etc., sofern magnetische Festplatten verwendet werden • kürzere Lebensdauer als z. B. Magnetbänder
Bandlaufwerke	• günstiger Preis für sehr hohe Kapazität • wenig Energiebedarf • lange Lebensdauer • Trennung vom Netzwerk nach dem Speichern der Daten	• längere Sicherungs- und Wiederherstellungszeiten • komplizierte Bedienung
Storage-Systeme	• flexibel erweiterbar durch hohe Skalierbarkeit • hohe Speicherkapazität • hohe Übertragungsgeschwindigkeit	• wenn dauerhaft mit dem Netzwerk verbunden, dann leicht angreifbar
Cloud-Speicher	• flexibel erweiterbar durch hohe Skalierbarkeit • einfache Art der Auslagerung der Daten aus dem lokalen Standort • keine eigene Hardware notwendig • unabhängig vom Standort (von überall aus zugreifbar)	• Transferrate hängt von der Internet-Bandbreite ab • Kontrollverlust über eigene Daten durch Auslagerung an externen Anbieter • Verschlüsselung erforderlich

Tabelle 2: Vor- und Nachteile von unterschiedlichen Speichermedien [BIT2016], [BRE2022], [NIST2020]

Die Gegenüberstellung der Speichermedien in der Tabelle 2 macht deutlich, dass optische Datenträger aufgrund niedriger Speicherkapazitäten sowie der Anfälligkeit für Hardwareschäden bei Stürzen oder Erschütterungen für die Datensicherung eher ungeeignet sind. Der einzige Vorteil besteht im günstigen Preis, allerdings besteht dieser Vorteil auch bei den mobilen Wechseldatenträgern. Diese haben zudem eine höhere Speicherkapazität gegenüber den optischen Datenträgern, sind aber ebenfalls empfindlich gegenüber Stürzen und Erschütterungen, sofern es sich um klassische Festplattenlaufwerke handelt und eignen sich daher eher für weniger umfangreiche Datensicherungen in kleineren Unternehmen. Für komplexere Datensicherungslösungen bieten sich die anderen drei betrachteten Speichermedien an. Die Sicherung auf Band überzeugt dabei vor allem durch einen niedrigen Preis pro Speicherplatz und die zuverlässige, langfristige Speicherung mit hoher Kapazität. Bei hohen Verfügbarkeitsanforderungen sind weiterhin Storage-Systeme wie beispielsweise Network Attached Storage (NAS) eine gute Option, da sich diese direkt im Unternehmensnetzwerk befinden und eine hohe Übertragungsgeschwindigkeit aufweisen. Abschließend eignet sich die Cloud für Datensicherungslösungen in jeder Größe, da diese flexibel und bezüglich des erforderlichen Speicherplatzes einfach erweiterbar ist. Zudem bietet die Cloud eine Möglichkeit, seine Daten extern auszulagern. Wichtig hierbei ist allerdings, den richtigen Anbieter auszuwählen, welcher die erforderlichen Datenschutzbestimmungen einhält, um das Risiko des Kontrollverlustes über die eigenen Daten zu minimieren. Grundsätzlich gilt bei der Datensicherung in einer Cloud deswegen, dass die Daten bereits vor der Auslagerung verschlüsselt werden sollten [BSI2023a], [BRE2022], [NIST2020].

Folgende Punkte sind bei der Nutzung von Cloud nach [BSI2023a] besonders zu beachten:

- An welchem Ort (Land) erfolgt die Datenspeicherung. In diesem Kontext ist besonders auf die DSGVO sowie der damit einhergehenden Herausforderungen bei Speicherorten außerhalb der EU zu achten. Siehe hierzu [EPR2016]
- Vereinbarung einer Dienstgüte (engl. Service Level Agreement, SLA) insbesondere im Hinblick auf die Verfügbarkeit
- Bietet der Cloudanbieter geeignete Authentisierungsmethoden (z. B.: Benutzerkennung und Passwort, Token, Authenticator-App, etc.)
- Möglichkeiten zur Verschlüsselung der Daten auf dem Online-Speicher
- Möglichkeiten zur Verschlüsselung auf dem Transportweg

4.4 Aufbewahrungsort

Bezüglich des Aufbewahrungsortes sollten die Speichermedien mit den darauf befindlichen Datensicherungen in einem anderen Brandabschnitt gelagert werden als die IT-Systeme mit den Produktivdaten. Ist dies nicht realisierbar, beispielsweise bei Kleinstunternehmen, so sollten die Datensicherungen außer Haus gelagert werden. In diesem Fall ist darauf zu achten, dass die Datensicherungen vor der Mitnahme verschlüsselt werden. Weiterhin muss der letztendlich ausgewählte Aufbewahrungsort über die notwendigen klimatischen Bedingungen verfügen, sodass die Speichermedien dort auch über einen längeren Zeitraum problemlos gelagert werden können. Herrscht dort beispielsweise eine sehr hohe Temperatur, könnte dadurch die Lebensdauer des Speichermediums beeinträchtigt werden. Außerdem sollte ein physischer Schutz der Datensicherungen bestehen, beispielsweise durch einen abschließbaren Schrank und/ oder eine Zutrittskontrolle, bei der nur berechtigte Personen den Zugang in den entsprechenden Raum erhalten.

4.5 Zuständigkeiten und Pläne

In den Unterkapiteln dieses Kapitels wird auf die wichtige Funktion des/der Datensicherungsbeauftragten sowie die Wichtigkeit eines Notfallplans und von Wiederherstellungstests eingegangen.

4.5.1 Datensicherungsbeauftragte*r

Im Bereich Zuständigkeiten muss festgelegt werden, wer für die Durchführung der Datensicherungen zuständig ist. Dazu gehört auch die Überwachung, dass die Durchführung ohne Fehlermeldungen erfolgt und die Vorgaben des Datensicherungskonzeptes eingehalten werden. Im Falle der Abwesenheit oder des Nichterreichens der zuständigen Person(en), muss eine vertretende Person festgelegt werden. Besonders bei hohen Integritäts- oder Vertraulichkeitsanforderungen muss klar geregelt sein, welche Personen Zugang zu den Datensicherungen haben dürfen. Außerdem sollte auch festgelegt werden, wer die Befugnis erhält, eine Wiederherstellung des gesamten Datenbestandes bzw. einzelner Dateien zu veranlassen und wer die Befugnis hat, diese durchzuführen.

4.5.2 Notfallplan

Der Notfallplan (engl. Disaster-Recovery-Plan) eines Unternehmens beinhaltet unter anderem die Vorgehensweise der Wiederherstellung im Falle eines Datenverlustes. Hierbei werden Vorgaben, Verfahren und Maßnahmen beschrieben, welche im Notfall schrittweise abgearbeitet werden müssen. Neben dem weiter oben bereits erwähnten Recovery Point Objective, ist beim Disaster Recovery das Recovery Time Objective (RTO) eine weitere wichtige Kenngröße. Das RTO ist eine Vorgabe, wie lang die maximale Ausfallzeit eines IT-Systems sein darf. Nach Ablauf dieser Zeit muss das System entsprechend wieder vollständig hergestellt sein. Weiterhin kann im Notfallplan festgelegt werden, in welcher Reihenfolge IT-Systeme oder auch Anwendungen wiederhergestellt werden müssen. Hierbei sollten geschäftskritische Systeme zuerst berücksichtigt werden [LUS2018],

[BSI2023a]. Unterstützenden Material zum Erstellen eines Notfallplans bietet die Allianz für Cybersicherheit unter [AFC2021] an.

4.5.3 Wiederherstellungstests

Neben der Notfallplanung ist eine weitere elementare Anforderung bezüglich Datensicherungen das regelmäßige Testen der Wiederherstellung der Daten. Auf diese Weise wird sichergestellt, dass die Wiederherstellung im Notfall ohne Probleme und auch innerhalb der Zeitvorgaben funktioniert. Hierbei ist auch zu prüfen, wie lange eine Wiederherstellung benötigt. Bei unzureichender Wiederstellungsgeschwindigkeit können so bei Bedarf noch Optimierungen vorgenommen werden. Werden die regelmäßigen Tests vernachlässigt, können eventuell auftretende Fehler bei der Wiederherstellung nicht erkannt werden. Treten diese Fehler dann im Ernstfall auf, könnte dies zu Datenverlust und weiteren erheblichen Schäden führen. Es kann außerdem vorkommen, dass die Datensicherung für eine Wiederherstellung gar nicht verwendet werden kann, da die Datensicherung fehlerhaft durchgeführt wurde.

Bei der Durchführung der Wiederherstellungstests sollte durch eine Überprüfung der Datensicherungs-Daten sichergestellt werden, dass diese nicht bereits von einer Schadsoftware kompromittiert sind. Da Schadsoftware häufig nicht sofort erkannt wird, besteht die Möglichkeit, dass diese auch schon in den Datensicherungen enthalten ist. Weiterhin sollten die Daten im Testfall nicht im Aktivsystem wiederhergestellt werden, um bei einem auftretenden Fehler keine Schäden an der Produktivumgebung hervorzurufen. Stattdessen sollten Wiederherstellungstests an einem separaten System getestet werden. Hierbei ist zu beachten, dass dafür benötigte Datensicherungs-Hardware vorhanden und mit der primären Hardware der Produktivumgebung kompatibel sein muss.

5 Gliederungsvorschlag für eine Richtlinie zur Datensicherung

Richtlinien sind wichtige Dokumente, die Unternehmen bei der Durchführung von spezifischen Aufgaben unterstützen. Konkret können verschiedene Mitarbeitende mit Hilfe einer Richtlinie eine definierte Aufgabe durchführen. Das Resultat der durchgeführten Aufgabe ist hierbei identisch, unabhängig davon, welcher Mitarbeitende die Aufgabe mit Hilfe der Richtlinie durchführt. Gerade vor dem Hinblick der Wichtigkeit des Themas Datensicherung, sollte für diese Aufgabe eine schriftliche Richtlinie existieren. Hierbei sollte die Richtlinie mindestens folgende Punkte enthalten:

1. Dokumenteneigenschaften
2. Dokumentenhistorie
3. Einleitung
4. Geltungsbereich
5. Zweck
6. Regelungen
    a. Umfang der Datensicherung
    b. Durchführung der Datensicherung
    c. Aufbewahrung und Dokumentation der Datensicherung
    d. Aufbewahrungsort
    e. Funktionstest und Überprüfung der Wiederherstellbarkeit
    f. Gesetzliche Aufbewahrungs- und Löschfristen
7. Anhang

Der Gliederungsvorschlag der Richtlinie orientiert sich an [LSI2022]. Detaillierte Ausführungen zu den einzelnen Punkten sind im Original beschrieben und dienen als Vorlage. Weiterhin stellt das Landesamt für Sicherheit in der Informationstechnik eine Tabelle zur Verfügung, mit Hilfe dessen Datensicherungen geplant und dokumentiert werden können. Die Tabelle finden Sie unter [LSI2021].

6 Schadsoftware-Resilienz für Datensicherungen

Zum Schutz gegen Schadsoftware müssen Datensicherungen so angelegt sein, dass sie für die Schadsoftware auch im Fall einer Kompromittierung eines Arbeitsplatzrechners oder eines Dateiservers für den Angreifer nicht zu erreichen sind. Hierzu wird zunächst der Ablauf eines Angriffs durch einen Verschlüsselungstrojaner beschrieben, bevor anschließend Schutzmaßnahmen erläutert werden.

6.1 Beschreibung eines Verschlüsselungstrojaner-Angriffs

Der folgende Ablaufplan zeigt das Vorgehen eines Angriffs durch Verschlüsselungstrojaner. Hierbei werden die einzelnen Phasen des Angriffs, inklusive der manuellen Steuerung des Verschlüsselungstrojaners, z. B. durch einen Fernzugriff, grob dargestellt. Die Übersicht orientiert sich hierbei am Leitfaden [LSI2023]:

1. Aufklärungsphase: Angreifende sammeln in dieser Phase Informationen über das Unternehmen sowie potenzielle Ziele.
2. Eindringphase: In dieser Phase schaffen sich die Angreifenden einen Zugang in die Systeme über mögliche Einfallsvektoren, beispielsweise E-Mails oder Schwachstellen in IT-Systemen.
3. Ausbreitungsphase: Nach einem erfolgreichen Eindringen versuchen Angreifende auf weitere Systeme zuzugreifen und somit möglichst viele Systeme im Unternehmen zu kompromittieren.
4. Rechteausweitung: Angreifende versuchen möglichst hohe Rechte in einem System, beispielsweise einer Domain, zu erlangen.
5. Abgreifphase (optional): In dieser Phase werden wichtige Daten des Unternehmens vom Unternehmen zum Angreifenden ausgeleitet.
6. Verschlüsselungsphase: Das Unternehmen wird in dieser Phase aktiv verschlüsselt. Hierbei ist es möglich, dass ebenfalls die Datensicherungen verschlüsselt werden.
7. Erpressungsphase: Nach der Verschlüsselung erfolgt die Erpressung. Eine Entschlüsselung ist nur gegen eine Bezahlung, meist in Form von Kryptowährungen, möglich.
8. Zweite Erpressungsphase: Angreifende kommen nach einer erfolgreichen ersten Erpressung, bei der das Unternehmen Lösegeld bezahlt hat, in der Regel nach einiger Zeitpunkt zurück, um das Unternehmen ein zweites oder drittes Mal zu verschlüsseln und Lösegeld zu erpressen.

Zusätzlich zum Ablaufplan beinhaltet [LSI2023] einen Leitfaden in Form einer Checkliste für den Fall, das Unternehmen Opfer durch einen Angriff eines Verschlüsselungstrojaners geworden sind sowie Wiederherstellungsmaßnahmen und Aktivitäten, die nach einem Vorfall durchzuführen sind. Detaillierte Ausführungen zu den einzelnen Punkten sind im Original beschrieben und dienen als Vorlage.

6.2 Maßnahmen zur Umsetzung einer Schadsoftware-Resilienz

Im Folgenden werden verschiedene Maßnahmen beschrieben, die die Resilienz gegenüber Angriffen durch einen Verschlüsselungstrojaners signifikant erhöhen.

Bei der Nutzung eines zentralen Datensicherungs-Systems ist zu beachten, dass dieses während der Durchführung der Datensicherung eine Verbindung zum Unternehmensnetzwerk benötigt. Dennoch sollte auch hier verhindert werden, dass infizierte Arbeitsplatzrechner oder Dateiserver über einen Schreibzugriff auf das Datensicherungs-System verfügen. Schreibzugriffe ermöglichen es, Daten zu erstellen oder zu modifizieren. Neben Schreibzugriffen gibt es weitere alternative Zugriffsrechte. Eine Alternative ist der Lesezugriff, mit Hilfe dessen es möglich ist, Daten zu lesen und somit auf dessen Inhalte zuzugreifen. Eine Manipulation dieser oder das Erstellen von neuen Daten ist mittels Lesezugriff allerdings nicht möglich.

Push- und Pull-Datensicherung

Bei der Durchführung von Datensicherungen unterscheidet man zwischen Push- und Pull-Datensicherungen. Der Unterschied zwischen diesen beiden Methoden ist in Abbildung 6 auf der folgenden Seite dargestellt.

Bei einer Push- Datensicherung werden die zu sichernden Daten von der Quelle, beispielsweise einem Dateiserver

oder einem Computer, auf dem zu sichernden Daten liegen, auf die Datensicherungs-Systeme oder das entsprechende Speichermedium kopiert. Diese Methode setzt voraus, dass Quellsysteme über schreibende Zugriffsrechte für das Datensicherungs-System verfügen. Bei einer Kompromittierung durch Schadsoftware des Quellsystems kann diese nun ebenfalls die vorhandenen schreibenden Zugriffsrechte verwenden, mit Hilfe derer das Datensicherungs-System anschließend kompromittiert werden kann. Da dies verhindert werden soll, ist zur Erhöhung der Sicherheit die Pull-Methode vorzuziehen. Hierbei zieht sich ein Datensicherungs-System die zu sichernden Daten von den jeweiligen Quellsystemen. Auf diese Weise benötigt nur das Datensicherungs-System lesende Zugriffsrechte für die Quellsysteme. Die Quellsysteme hingegen benötigen keinerlei Zugriffsrechte, weder lesend noch schreibend, für das Datensicherungs-System. Bei einer Kompromittierung der Quellsysteme mittels Schadsoftware haben diese dementsprechend auch keinen Zugriff auf das Datensicherungs-System und können dieses nicht aktiv kompromittieren [VAH2020].

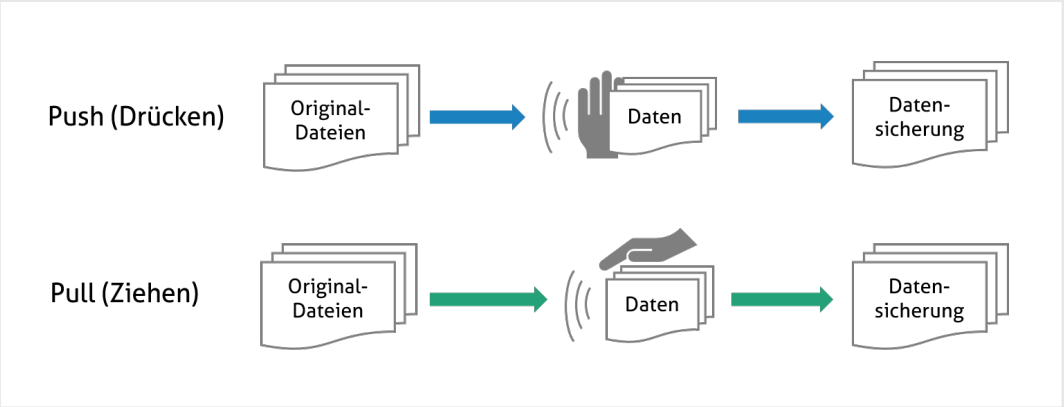


Abbildung 6: Push- und Pull-Datensicherungen

Unveränderliche Datensicherung

Weiterhin sollten auch die Speicher, auf denen die Datensicherungen abgelegt werden, einen Schutz gegenüber Kompromittierungen aufweisen. Neben einer physischen oder auch logischen Segmentierung von Datensicherungen gehört dazu auch die unveränderliche Speicherung. Hierbei sollte es sowohl für Administratoren als auch für eingeschränkte Benutzer unmöglich sein, die unveränderlichen Daten während eines festgelegten Aufbewahrungszeitraums zu löschen oder zu verändern. Für einen Verschlüsselungstrojaner, der über eine der genannten Rechte verfügt, ist es dann ebenfalls nicht möglich die unveränderlichen Daten zu kompromittieren.

Eine Möglichkeit zur Umsetzung beschreibt das WORM-Prinzip (write once, read many). Dieses Prinzip wird bei optischen Medien, beispielsweise CDs oder DVDs, verwendet. Nach einem Schreibvorgang auf den optischen Datenträgern ist eine erneute Veränderung der Daten nicht mehr möglich. Dieses Prinzip kann ebenfalls auf Serversysteme oder Cloudsysteme übertragen werden. Zu unterscheiden ist allerdings, dass anders als bei CDs oder DVDs, vor der durchzuführenden Datensicherung eine Zeitautomatik eingestellt werden kann, die eine Änderung der Daten nach einem festgelegten Zeitraum wieder ermöglicht. Diese Einstellung ermöglicht das Wiederverwenden von bereits belegtem Speicherplatz nach einer definierten Zeitspanne. Der freiwerdende Speicherplatz kann im Anschluss beispielsweise für neue und somit aktuellere Datensicherungen verwendet werden. Vor Ablauf der festgelegten Zeitspanne ist eine Änderung der Daten nicht möglich.

Allgemein ist darauf zu achten, dass der Unveränderlichkeitszeitraum weder zu klein noch zu groß gewählt wird. Ist er zu klein gewählt, ist der Schutz gegenüber Verschlüsselungstrojanern unzureichend. Ist er zu groß gewählt werden große Mengen an Speicherkapazitäten benötigt, da eine Wiederbeschreibung von Datenträgern, erst nach Ablauf des gewählten Zeitraums der Unveränderlichkeit wieder möglich ist. Außerdem sollte nach der Speicherung eine Verifikation stattfinden, welche sicherstellt, dass die Daten unbeschädigt und frei von Schadsoftware sind [DEL2022].

Zusammenfassung

In diesem Kapitel wurden die wichtigsten Eigenschaften von Datensicherungen beschrieben, um eine Resilienz gegenüber Angriffen durch Verschlüsselungstrojaner zu erreichen. In der folgenden Aufzählung (Tabelle 3) werden die zwei wichtigsten Anforderungen nochmal herausgestellt.

Pull-Datensicherung:
Verwenden Sie zum Durchführen der Datensicherungen die Pull-Datensicherung, um zu verhindern, dass Verschlüsselungstrojaner mit Hilfe von schreibenden Zugriffsrechten vorhandene Datensicherungen kompromittieren können.

Unveränderliche Datensicherung:
Verwenden Sie unveränderliche Datensicherungen, damit im Falle eine Kompromittierung des Unternehmens, die Datensicherungen vor einem Verschlüsselungstrojaner geschützt sind.

Tabelle 3: Anforderungen an Schadsoftware-resiliente Datensicherungen

In den kommenden Kapiteln folgen auf Basis der dargestellten Grundlagen, Voraussetzungen sowie der Schadsoftware-Resilienz praktische Beispiele zur Umsetzung einer Verschlüsselungstrojaner-resilienten Datensicherung. Hierzu werden zunächst Anforderungen zusammengefasst, bevor anschließend das Konzept vorgestellt wird.

7 Anforderungen an eine Verschlüsselungstrojaner-resiliente Datensicherung

Um eine Resilienz gegenüber Verschlüsselungstrojanern im Unternehmen herzustellen und aufrechtzuerhalten, gilt es Anforderungen in Bezug auf Datensicherungen umzusetzen. Folgende Anforderungen, die in den vorrangegangenen Kapiteln erläutert wurden, müssen mindestens erfüllt werden:

- Die 3-2-1-Regel muss eingehalten werden.
- Durch ein geeignetes Rotationsschema sollten tägliche, wöchentliche und monatliche Datensicherungen erstellt werden.
- Vollsicherungen sollten durch inkrementelle Sicherungen ergänzt werden.
- Es sollten je nach Bedarf mehrere monatliche Sicherungen aufbewahrt werden. Dementsprechend muss ausreichend Speicherplatz vorhanden sein.
- Die Durchführung der Datensicherungen sollte angemessen dokumentiert werden.
- Es sollten regelmäßige Wiederherstellungstests durchgeführt und dokumentiert werden. Diese sollten nicht auf dem Quellsystem stattfinden.
- Die Datensicherungen müssen gegen Ransomware geschützt sein. Hierbei bietet es sich an Pull-Datensicherungen durchzuführen sowie die Speichermedien nur zu den Sicherungszeitpunkten mit dem Netzwerk zu verbinden.
- Für die Datenspeicherung sollten unveränderliche Datensicherungen verwendet werden.
- Die Datensicherungen sollten bei der Lagerung je nach Vertraulichkeitsbedarf verschlüsselt gespeichert werden, insbesondere bei Lagerung außer Haus oder in der Cloud.
- Die Datensicherungen können bei der Lagerung zur Reduzierung des benötigten Speicherplatzes in komprimierter Form gespeichert werden.
- Die Gesamtkosten müssen sich innerhalb eines angemessenen Rahmens befinden.
- Datensicherungen, die in der Cloud abgelegt werden, sollten verschlüsselt sein. Zudem sollte eine Cloud-Lösung die Versionierung der Datensicherungen unterstützen.

8 Best Practice: Konfigurations- und Schutzmaßnahmen für eine Verschlüsselungstrojaner-resiliente Datensicherung

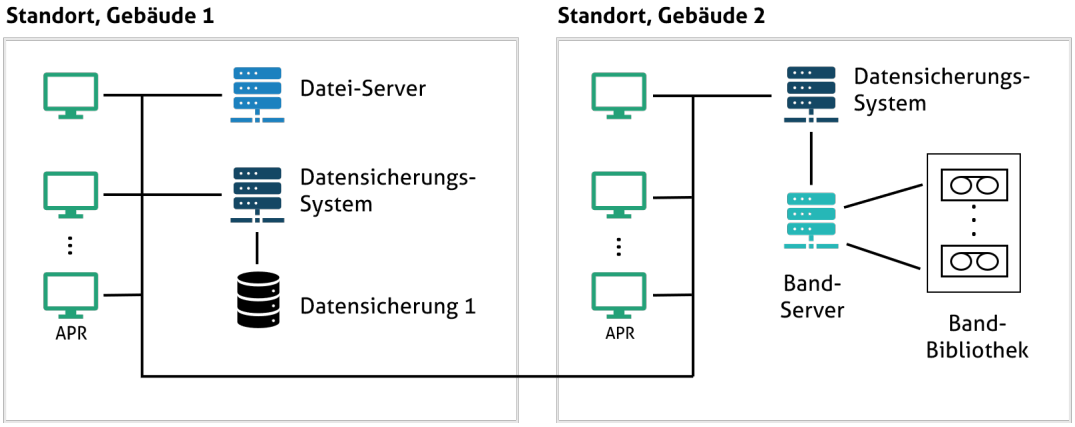


Abbildung 7: Datensicherungskonzept

Dieses Kapitel beschreibt ein mögliches Konzept zur Umsetzung für Verschlüsselungstrojaner-resiliente Datensicherungen. Das Konzept ist in Abbildung 7 dargestellt.

Das Konzept besteht aus einer Netzwerkinfrastruktur, die hier zur besseren Übersicht vereinfacht dargestellt ist. Weitere Netzwerkteilnehmer, wie beispielsweise Drucker, Switche, Firewalls oder weitere Server sind nicht dargestellt. Stattdessen wird sich auf die für Datensicherungen notwendige Infrastruktur konzentriert. Die Gebäude eins und zwei sind so weit voneinander entfernt, sodass sie jeweils einen anderen Brandabschnitt darstellen. Im Konzept sind folgende Komponenten vorhanden:

APR
In jedem Gebäude des Standorts arbeiten die Mitarbeitenden auf Arbeitsplatzrechnern (APR). Alternativ zu APR können beispielsweise auch Server verwendet werden, die als Hosts für virtuelle Maschinen (VM) dienen. Die Mitarbeitenden arbeiten in diesem Fall jeweils auf einer der gehosteten VMs.

Datei-Server
Auf dem Datei-Server werden die Produktivdaten durch die Mitarbeitenden abgelegt sowie vom Server für die weitere Bearbeitung abgerufen. Diese Daten gilt es mit Hilfe des Datensicherungskonzepts abzusichern.

Datensicherungs-System
An jedem Standort befindet sich mindestens ein Datensicherungs-System, auf welchem die Datensicherungs-Software installiert ist. Diese dient als zentrales Element für die Konfiguration und Kontrolle der Datensicherungen. Außerdem finden hier die Planung und Erstellung der Datensicherungs- und Wiederherstellungsaufträge statt. Wichtig ist, dass die Software zum Durchführen von Datensicherungen ebenfalls mit Hilfe der Unveränderlichkeit (siehe 6 Schadsoftware-Resilienz für Datensicherungen) geschützt ist. Teil des Datensicherungs-Systems kann ebenfalls, gerade bei großen Unternehmen, ein Datensicherungs-Proxy sein, der dazu dient, die von der Datensicherungs-Software verwalteten Aufgaben auszuführen. Dazu gehört das Abrufen der zu sichernden Daten aus der Produktivumgebung sowie das Senden der Daten zum Datensicherungs-Speicherort. Bei der Durchführung der Datensicherung ist darauf zu achten, dass die Pull-Methode (vgl. Kapitel 6 Schadsoftware-Resilienz für Datensicherungen) verwendet wird. Nur dann kann eine Resilienz gegenüber Verschlüsselungstrojanern gewährleistet werden. Weiterhin ist der Datensicherungs-Proxy für die Kompression, die Duplizierung und die Verschlüsselung der zu sichernden Daten zuständig.

Datensicherung
An jedem Standort befindet sich mindestens ein lokales Datensicherungs-System als Datensicherungs-Speicherort. Dieses bietet die Möglichkeit, die zu sichernden Daten unveränderlich zu speichern und somit zusätzlich gegenüber Verschlüsselungstrojanern zu schützen. Um dies zu ermöglichen kann beispielsweise das WORM-Prinzip verwendet werden.

Band-Server
Der Band-Server ist für die Datenübertragung zwischen der Quelle der zu sichernden Daten und den Bändern in der Band-Bibliothek notwendig. Alternativ kann auch das Datensicherungs-System gleichzeitig als Band-Server dienen. Wichtig ist, dass die Software des Band-Servers ebenfalls mit

Hilfe der Unveränderlichkeit (siehe 6 Schadsoftware-Resilienz für Datensicherungen) geschützt wird. Ein Verschlüsselungstrojaner hat sonst unter Umständen die Möglichkeit, die Software des Band-Servers zu verschlüsseln. Dies kann zur Folge haben, dass kein Zugriff mehr auf die Band-Bibliothek zur Verfügung steht, da der Band-Server für die Speicherung der Ablageorte von Bändern und Dateien zuständig ist.

Band-Bibliothek
In der Band-Bibliothek befinden sich mehrere Bänder, welche neben der Datensicherung 1 als weiterer Speicherort dienen. Wenn das Unternehmen über mehrere Standorte verfügt, kann, je nach Unternehmensgröße, eine einzige Band-Bibliothek für alle Standorte verwendet werden.

Cloud
Als zweites Datensicherungs-Ziel kann statt einem Band-Server die Cloud dienen, da diese eine alternative Möglichkeit für eine Offsite-Sicherung bietet.

Umsetzung der Datensicherungen
Außerdem ist die Konfiguration und Durchführung der Datensicherungen zu planen. Dies geschieht auf Basis von Kapitel 4 Technische und organisatorische Voraussetzungen für Datensicherungen sowie auf den in Kapitel 7 Anforderungen an eine Verschlüsselungstrojaner-resiliente Datensicherung aufgestellten Anforderungen an Datensicherungen. Die folgenden Punkte sind bezüglich der Datensicherungen umzusetzen:

- Datensicherungen sind täglich durchzuführen. Dabei ist eine wöchentliche Vollsicherung durchzuführen. An den restlichen Wochentagen ist jeweils eine inkrementelle Sicherung durchzuführen. Weiterhin ist eine monatliche Vollsicherung durchzuführen.
- Die Aufbewahrung der Datensicherungen findet gemäß dem in Kapitel 4.2 Anzahl Datensicherungsgenerationen beschriebenen Drei-Generationen-Prinzip statt, um eine effiziente Nutzung des Speicherplatzes zu gewährleisten.
- Der Zeitpunkt zum Durchführen der Datensicherungen sollte nach Ende der aktiven Arbeit sein, damit die Datensicherungen nachts und damit außerhalb des täglichen Betriebs stattfinden.
- Die Datensicherung 1 ist an jedem Standort in einem anderen Brandabschnitt als die Datei-Server zu platzieren, sofern keine Band-Bibliothek in einem anderen Brandabschnitt vorhanden ist. Außerdem ist sicherzustellen, dass die Räume mit den Speichermedien nicht durch Unbefugte zugänglich sind (z. B. durch das Abschließen der Räume).
- Die zu sichernden Daten des Datei-Servers sind redundant auf der Datensicherung 1 sowie in der Band-Bibliothek zu sichern. Dies gewährleistet die laut der 3-2-1-Regel benötigte Offsite-Sicherung am Standort, da sich die Datensicherungen 1 und die Band-Bibliothek in zwei verschiedenen Gebäuden befinden.
- Zur Information über Datensicherungs-Ergebnisse sind Benachrichtigungen per E-Mail zu konfigurieren, welche für die Datensicherungs-Aufträge die Zeitdauer sowie die Information sendet, ob der Auftrag erfolgreich, fehlerhaft oder mit einer Warnung ausgeführt wurde. Diese Benachrichtigungs-Mails sind an mehrere zuständige Personen zu senden, um zu verhindern, dass ein Fehler bei Abwesenheit einer Person unentdeckt bleibt.
- Die Wiederherstellbarkeit der Sicherungen ist regelmäßig zu testen. Außerdem sollten die Datensicherungen durch einen Malware-Scan überprüft werden.
- Bei der Sicherung auf Band ist für jede Woche und für jeden Monat ein eigenes Band zu verwenden. Es ist außerdem ein Aufbewahrungszeitraum festzulegen, welcher die Bänder vor Überschreiben schützt. Nach dem Fertigstellen des Sicherungsauftrags auf ein Band ist dieses offline zu nehmen.
- Alle durchzuführenden Handlungen und Konfigurationen sind ausführlich zu dokumentieren.

Zusätzliche Punkte bei mehreren Standorten
- Sollten mehrere Standorte vorhanden sein, so sind die zu sichernden Datei-Server an den Außenstandorten auf der Datensicherung 1 am jeweiligen Standort zu sichern sowie in der Band-Bibliothek am Standort der Abbildung 7. Auch hier ist durch die Auslagerung der Sicherungen an den Standort aus Abbildung 7 eine Offsite-Sicherung gewährleistet.
- Die Remote-Übertragung der Daten von den Außenstandorten an den Standort aus Abbildung 7 ist über eine sichere VPN-Verbindung durchzuführen.

Zusätzliche Maßnahme bei Cloud-Nutzung
- Die Cloud-Sicherung ist vor dem Ablegen in der Cloud quellseitig zu verschlüsseln.

9 Fazit

Verschlüsselungstrojaner sorgten in der Vergangenheit, sorgen aber auch aktuell, für große Schäden in Unternehmen. Diese können im schlimmsten Fall dazu führen, dass Unternehmen zahlungsunfähig werden. Deshalb ist es wichtig, dass Unternehmen sich vor Angriffen durch einen Verschlüsselungstrojaner aktiv schützen.

Aus diesem Grund bietet dieses Best Practice die Möglichkeit, Verschlüsselungstrojaner-resiliente Datensicherungen im Unternehmen einzuführen. Hierzu werden folgende Probleme bei Datensicherungen durch das Best Practice adressiert:

1. Datensicherungen sind im Unternehmensnetzwerk direkt eingebunden.
2. Moderne Verschlüsselungstrojaner versuchen neben den Aktivdaten ebenfalls vorhandene Datensicherungen zu kompromittieren.
3. Notwendiges Knowhow ist in Unternehmen zum Teil nicht in ausreichender Menge vorhanden.

Quelle: Alexander Limbach/stock.adobe.com

10 Verzeichnisse

10.1 Abbildungsverzeichnis

10.2 Tabellenverzeichnis

10.3. Literaturverzeichnis

[AFC2021]
Allianz für Cybersicherheit: Massnahmen-Katalog zum Notfallmanagement. Fokus IT-Notfälle.

[BIT2016]
Bitkom e. V.: Backup / Recovery / Disaster Recovery. URL: https://www.bitkom.org/sites/default/files/file/import/170125-LF-Backup-Recovery.pdf.

[BIT2022]
Bitkom e. V.: 203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen. URL: https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022.

[BRE2022]
BREKOM GmbH: Datensicherung – Warum Backups so wichtig sind, wie sie lückenlos funktionieren. URL: https://brekom.de/ratgeber-it-sicherheit/datensicherung/, 10.07.2023.

[BSI2022a]
Bundesamt für Sicherheit in der Informationstechnik: Umsetzungshinweise zum Baustein CON.3 Datensicherungskonzept. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2022/Umsetzungshinweis_zum_Baustein_CON_3_Datensicherungskonzept.pdf?__blob=publicationFile&v=2 - download=1.

[BSI2022b]
Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2022. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6.

[BSI2022c]
Bundesamt für Sicherheit in der Informationstechnik: Ransomware Bedrohungslage 2022. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?__blob=publicationFile&v=2.

[BSI2022d]
Bundesamt für Sicherheit in der Informationstechnik: Maßnahmenkatalog Ransomware. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Massnahmenkatalog.pdf?__blob=publicationFile&v=2.

[BSI2023a]
Bundesamt für Sicherheit in der Informationstechnik: CON.3 Datensicherungskonzept. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/03_CON_Konzepte_und_Vorgehensweisen/CON_3_Datensicherungskonzept_Edition_2023.pdf?__blob=publicationFile&v=3#download=1, 11.07.2023.

[DEL2022]
Dell Technologies: Recovering from a Cyber Event. URL: https://www.delltechnologies.com/asset/de-de/products/data-protection/industry-market/dell-powerprotect-cyber-recovery-recover-from-cyber-event-wp.pdf.

[DIN_EN_ISO_27000]
Deutsches Institut für Normung e. V.: DIN EN ISO/IEC 27000:2020 Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Überblick und Terminologie (ISO/IEC 27000:2018), 2020, Jahrgang Deutsche Fassung EN ISO/IEC 27000:2020.

[EPR2016]
Europäisches Parlament und des Rates: Europäische Datenschutz-Grundverordnung. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE.

[LSI2021]
Landesamt für Sicherheit in der Informationstechnik: Planung der Backup-Durchführung. URL: https://www.lsi.bayern.de/mam/aktuelles/backup_dokumentation.xlsx, 18.10.2023.

[LSI2022]
Landesamt für Sicherheit in der Informationstechnik: Backup-Richtlinie. URL: https://www.lsi.bayern.de/mam/aktuelles/backup-richtlinie.docx, 18.10.2023.

[LSI2023]
Landesamt für Sicherheit in der Informationstechnik: LSI-Leitfaden. Ransomware. URL: https://lsi.bayern.de/mam/aktuelles/ransomware_leitfaden_v1_2.pdf, 18.10.2023.

[LUS2018]
Luber, S.; Schmitz, P.: Was ist Disaster Recovery? URL: https://www.security-insider.de/was-ist-disaster-recovery-a-732206/, 17.07.2023.

[MS2022]
Morgan, Steve; Sausalito, Calif: Die drei grössten Ransomware-Trends 2021. IT-Sicherheit-Edition April/Mai 2/2022, 2022; S. 26-27. URL: https://www.datakontext.com/EPaper/index/active/1/epaper/17696.

[NIST2020]
National Institute of Standards and Technology: Protecting data from ransomware and other data loss events. A Guide for Managed Service Providers to Conduct, Maintain and Test Backup Files. URL: https://www.nccoe.nist.gov/sites/default/files/legacy-files/msp-protecting-data-extended.pdf, 13.07.2023.

[VAH2020]
Vahldieck, A.: Emotet: Hält Ihr Backup? So sichern Sie ihre Daten wirklich zuverlässig. In c't Magazin für Computertechnik-Edition, 10/2020, 2020; S. 16–21.

Kontakt für Rückfragen

Prof. Dr. Karl-Heinz Niemann
0511 929 612 64
karl-heinz.niemann@hs-hannover.de

Mittelstand-Digital
Zentrum
Hannover