RANSOMWARE-SICHERE BACKUPS – HILFE ZUR SELBSTHILFE

Umsetzungsmöglichkeiten

Stand: Version 1.1, 19.03.2021, 10:00 Uhr
Quelle/ggf. aktualisierte Versionen:
research.hisolutions.com/2021/03/schutz-gegen-ransomware-hisolutions-selbsthilfe-offline-backup/

SACHVERHALT

Ransomware ist und bleibt die größte Bedrohung für Unternehmen und öffentliche Einrichtungen. Alle Daten eines digitalen Systems können im Angriffsfall verschlüsselt werden – das schließt Sicherungskopien mit ein. Häufig werden diese sogar zuerst vom Angreifer gelöscht, gesperrt oder manipuliert.

Beim klassischen Backup ist das oberste Ziel die schnelle Wiederherstellbarkeit für „normale“ Fehlfunktionen, daher sind die Backup-Daten oft „live“ im Zugriff durch die IT-Infrastruktur – und damit auch durch den Angreifer. Ein Ransomware-sicheres Backup verweigert dem Angreifer diesen Zugriff.

ANFORDERUNGEN

Die Anforderungen, welches ein Ransomware-sicheres-Backup erfüllen muss, sind:

- Die Backup-Daten dürfen nicht im Zugriff der zu sichernden Systeme liegen.
- Die Backup-Daten dürfen nicht mit Domänenberechtigungen erreichbar sein.
- Die Backup-Daten dürfen nicht mit denselben Kennwörtern, die auch in der Domäne verwendet werden, erreichbar sein.

Sind diese Anforderungen nicht erfüllt, kann ein Angreifer Zugriff auf die Daten erhalten. In typischen Fällen werden nicht nur einzelne Systeme, sondern komplette Domänen kompromittiert und mit den erhaltenen Rechten gezielt nach Backups gesucht.

LÖSUNGSMÖGLICHKEITEN

Klassische Offline-Backups

Die einfachste Möglichkeit bösartige Zugriffe zu unterbinden, besteht in einem Offline-Backup, d. h. einem Backup, bei dem die Speichermedien außerhalb des Zugriffs der IT-Infrastruktur aufbewahrt werden. Offline-Backups bieten eine hohe Sicherheit gegenüber externen Zugriffen, haben aber in der Zugriffsgeschwindigkeit oft Nachteile, weshalb sie oft als zweite Ebene eines schnelleren Konzepts gefahren werden.

HiSolutions AG
Schloßstraße 1
12163 Berlin

info@hisolutions.com
www.hisolutions.com

+49 30 533 289-0
+49 30 533 289-900

Option 1: Externe Festplatte

Die einfachste Art und Weise, Dateien zu sichern, ist die Verwendung externer Festplatten. Gerade in kleinen Betrieben kann dies eine wirtschaftliche Lösung sein. Hierbei werden die Dateien als Sicherungskopien vom ursprüglichen Speichermedium üblicherweise via USB-Verbindung auf den externen Datenträger kopiert. Andere Technologien wie FireWire, Thunderbolt und eSATA sind ebenfalls gebräuchlich.

Vermeiden Sie typische Fehler**:** Da zumindest temporär eine Verbindung zum System vorhanden ist, müssen immer zeitlich gestaffelt mehrere Medien im Umlauf sein, sodass im Schadensfall nur die aktuelle Generation betroffen ist. Rechnen Sie auch damit, dass eine Verschlüsselung durch Ransomware u. U. über Wochenende oder Feiertage zunächst ein oder auch zwei Tage unbemerkt bleibt, bevor die Backups gestoppt werden.

Option 2: Bandsicherung (Tape)

Bei einer Bandsicherung werden in regelmäßigen Abständen alle oder definierte Daten von einem digitalen Datenträger auf ein Magnetband übertragen. Außerhalb von Lese- oder Schreibvorgängen sind auf Bändern gespeicherte Daten nicht mit dem Netzwerk verbunden. Die auf LTO (Linear Tape Open) gespeicherten Datenkopien gehen nur dann online, wenn der Notfall eintritt und mit ihnen gearbeitet werden muss. Die Bänder können dafür jederzeit aus der Bibliothek entnommen werden. Die Verwendung von Tapes stellt eine effektive und kostengünstige Methode dar. Zudem sollte ein Teil der Tapes immer außerhalb des Systems aufgewahrt werden.

Vermeiden Sie typische Fehler**:**

- Prüfen Sie, ob die Bänder auch dann einsatzfähig sind, wenn die am Netz befindlichen Backup-Server vom Angreifer gelöscht oder betriebsunfähig gemacht wurden.
- Halten Sie Boot-Medien für die für das Recovery benötigten Server bereit und planen Sie eine Methode zur Bare-Metal-Recovery für die Backup-Server und alle benötigten Infrastruktursysteme (z. B. Domänencontroller).
- Bandroboter halten oft den Index der gespeicherten Dateien online verfügbar – prüfen Sie, was passiert, wenn dieser Index nicht mehr verfügbar ist. Können Sie die Bänder mit den benötigten Inhalten dann noch schnell genug identifizieren?
- Proben Sie die vollständige Recovery bei zerstörten Backup-Servern.

Option 3: WORM-Medien (Write-Once-Read-Many)

Bei WORM-Speichermedien handelt es sich um Speichermedien, auf denen Daten einmalig abgespeichert und nicht mehr verändert werden können. Das Lesen ist beliebig oft möglich. Als Speichermedium wurden früher häufig CDs oder DVDs genutzt. Für aktuelle Datenmengen sind diese jedoch bis auf Nischenanwendungen ungeeignet.

Bei neueren als WORM angebotenen Lösungen handelt es sich praktisch immer um eine Hardware-Kombination aus Festplatte/SSD mit speziellen Firmwares, die den „Write-Once“-Aspekt ohne Eingriffsmöglichkeit des Systems in eingebetteter Software, sicherzustellen versuchen. Hier zielen die Produkte vor allem auf einen Nischenmarkt mit hohen regulatorischen Anforderungen.

Hybride Verfahren auf NAS-Systemen/Backup-Servern

Network Attached Storage Systeme (NAS) werden oft für Online-Sicherungsverfahren verwendet. Leider wird das Backup häufig über Freigaben der NAS-Systeme durchgeführt, die für Windows-Domänennutzer zugänglich sind. Alternativ werden NAS- oder SAN-Systeme einem vorgeschaltete Backup-Server nachgelagert.

Um den Einsatz von NAS-Systemem sicher gegen Ransomware Angriffe zu machen, existieren mehrere Möglichkeiten:

Option 4: Zusätzliche Backups auf externe Festplatten

NAS-Systeme können häufig über extern angebundene Festplatten (z. B. über USB) automatisiert gesichert werden, die im Rahmen eines regelmäßigen (z. B. täglichen) Rotationsverfahrens leicht auszuwechseln und sicher zu hinterlegen sind. Hier gilt dasselbe wie bei Option 1.

Vermeiden Sie typische Fehler**:** Die Festplatten dürfen nicht dauerhaft am NAS-System angeschlossen bleiben, da sie sonst ebenfalls überschrieben werden können. Daher sollten Sie mindestens zwei Festplatten nutzen und diese rotieren.

Option 5: Pull-Verfahren durch Backup Server/NAS-System

Das Pull-Verfahren basiert immer auf einer Backup-Software, die den Kontakt vom Backup-Server/NAS-System zu einem Agenten auf den Client-Systemen aufbaut und sich von diesen das Backup „zieht“. Dabei hat der Client keinen Zugriff auf die Inhalte des Backup-Servers, nur der Backup-Server auf den Client. Die Umsetzung ist stark abhängig von der eingesetzten Backup-Software und den gewählten Transfermethoden.

Vermeiden Sie typische Fehler**:**

- Auf dem NAS-System / dem Backup-Server sind durch diese Art der Automatisierung Zugangskennungen für alle im Backup befindlichen Systeme vorhanden, sodass bei einer Kompromittierung des Backup-Servers sofort Zugriff auf sämtliche Systeme möglich ist. Der Backup-Server muss entsprechend abgesichert werden.
- Überprüfen Sie, wie Ihre Backup-Software den Zugriff realisiert – oft werden trotzdem erreichbare Freigaben eingesetzt, zudem sind die eingesetzten Mechanismen häufig nicht transparent.
- Das NAS-System darf in diesem Fall nicht Mitglied der Domäne sein; dies erschwert aber die Verwaltung und den Einsatz enorm. Nicht jede Backup-Software unterstützt zudem einen solchen Betrieb.
- Auf dem NAS-System dürfen keine Kennungen und Passworte eingesetzt werden, die ebenfalls in der Domäne verwendet werden.
- Die Administration sollte nicht von einem System innerhalb der Domäne durchgeführt werden, da dort die Passwörter abgegriffen werden könnten. Hier kann ein separater Laptop zusätzlichen Schutz bringen.

Achtung: Diese Option ist in der Umsetzung oft fehlerträchtig.

Option 6: NAS-Snapshots

Viele NAS-Systeme unterstützen Snapshots – entweder Dateisystem-basiert oder blockbasiert. Wird ein Snapshot angelegt, werden darauffolgende Änderungen als Differenz separat abgespeichert, sodass jederzeit zum ursprünglichen Zustand beim Snapshot zurückgekehrt werden kann. Es können auch mehrere Snapshots angelegt werden. Bei einer Konfiguration für das Backup sollten üblicherweise Snapshots automatisiert in bestimmten Zeitabständen angelegt werden.

Diese Möglichkeit kann genutzt werden, um auch bei einem NAS-System mit einer Freigabe im Domänenzugriff sicherzustellen, dass von einem Angreifer keine Daten gelöscht werden können.

Vermeiden Sie typische Fehler**:**

- Der Zugriff auf die angelegten Snapshots darf nicht für Domännennutzer freigegeben sein.
- Der administrative Zugriff auf das NAS-System darf nicht mit einer in der Domäne vorhandener Kennung erfolgen, auch nicht mit gleichlautendem Passwort.
- Der notwendige Speicherplatz sollte mit Sicherheitsabstand kalkuliert werden: Der Speicherbedarf jedes Snapshots kann zwischen „fast null“ und „vollem Speicherplatz“ variieren, je nach Größe der Änderungen. Bei einem Ransomware-Angriff wird der Speicherbedarf maximal groß werden, da alle Daten geändert werden.
- Die Snapshots dürfen beim Erreichen der maximalen Kapazität auf keinen Fall automatisch gelöscht werden – in diesem Fall sollte vorher eine Fehlermeldung/Alarm abgesetzt und der Schreibzugriff notfalls gesperrt werden.
- Bei sehr vielen aktiven Snapshots kann die Performance des NAS beeinträchtigt werden – prüfen Sie die Dokumentation Ihres Systems.
- Die Administration sollte nicht von einem System innerhalb der Domäne durchgeführt werden, da dort die Passwörter abgegriffen werden könnten. Hier kann ein separater Laptop zusätzlichen Schutz bringen.

Option 7: Kaskadierende NAS

Ein kaskadiertes Sicherungsverfahren über zwei NAS-Systeme ist ebenfalls möglich. Bei der Umsetzung ist darauf zu achten, dass nur ein NAS-System (NAS1) direkt als Online-Sicherungsverfahren genutzt wird. Das zweite NAS (NAS2) sollte sich die Backups vom NAS1 zyklisch (z. B. täglich) abholen – wie bei Option 5, allerdings sind hier Bordmittel wie „rsync“ möglich und häufig genutzt. Ansonsten gelten alle Bedingungen und Hinweise von Option 5.

Eine zweite Möglichkeit ist die Konfiguration des zweiten NAS-Systems mit Hilfe von Snapshots wie bei Option 6.

Vorteilhaft an dieser Option ist die Möglichkeit, durch das zweite NAS auch gleichzeitig eine höhere Standortredundanz zu erlangen.

Vermeiden Sie typische Fehler**:**

- Bei der Absicherung der beiden NAS-Systeme ist darauf zu achten, dass unterschiedliche Benutzerkonten und Passwörter verwendet werden.
- Für eine höhere Sicherheit sollten Sie bei der Netzintegration darauf achten, die Zugriffe auf das zweite NAS stark zu reglementieren.
- Ansonsten gelten die Hinweise von Option 5 bzw. 6.

Option 8: Cloud Backup

Neben einer rein lokalen Speicherung von Daten kann zudem erwogen werden, bestimmte Daten in eine Cloud-Storage-Umgebung zu sichern. Für diese Art der Datensicherung benötigen Sie in der Regel eine spezielle Software, die entweder vom Anbieter des Backup-Services selbst stammt oder aber dessen API bedienen kann.

Bei diesem Sicherungsverfahren sind neben dem benötigten Speicherbedarf auch Gegebenheiten wie etwa die verfügbare Bandbreite und Fragestellungen der Datensicherheit bzw. des Datenschutzes sowie sonstiger Compliance zu berücksichtigen.

Auch bei einem hybriden Sicherungsverfahren in einen Cloud-Storage muss durch Zugriffskontrollen und Versionierungsverfahren darauf geachtet werden, dass die gesicherten Daten nicht von zu sichernden Systemen aus modifiziert oder gelöscht werden können.

Bei Cloud-Umgebungen ist eine Pull-Lösung im Regelfall nicht möglich (und auch nicht sinnvoll). Daher muss die Sicherheit durch Snapshot-Technik wie bei Option 6 oder durch eine Backup-spezifische dedizierte Lösung sichergestellt werden.

Vermeiden Sie typische Fehler**:**

- Der Zugriff auf die gesicherten Cloud-Daten (Snapshots) darf nicht mit Hilfe der auf den Systemen genutzten Zugangsdaten (API-Keys, Kennungen, Passwörter) möglich sein.
- Der administrative Zugriff auf die Backup-Daten darf nicht über ein Domänenbenutzerkonto oder eine Federation erreichbar sein.
- Jeglicher Zugriff auf gesicherte Backup-Daten (Snapshots) sollte ausschließlich über Konten mit Mehr-Faktor-Authentifizierung (MFA) möglich sein.
- Die Verfügbarkeit der Cloud-Backups sollte regelmäßig überprüft werden.

RANSOMWARE-SICHERE-BACKUPS ALS TEIL IHRES DATENSICHERUNGSKONZEPTS

Ransomware-sichere Backups sollten integraler Bestandteil eines jeden ganzheitlichen Datensicherungskonzepts sein. Ein solches Konzept muss an den Erfordernissen der jeweiligen Organisation unter Berücksichtigung tolerierbarer Ausfallzeiten und akzeptabler Wiederherstellungszeiten ausgerichtet sein. Zwischen Organisationen können sich die Anforderungen in Bezug auf Sicherungshäufigkeit, -verfahren und Aufbewahrung stark unterscheiden. Bei der Umsetzung empfiehlt es sich häufig, eine geeignete Kombination aus verschiedenen der in diesem Dokument dargestellten Backup-Verfahren einzusetzen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit dem Baustein „CON.3: Datensicherungskonzept“ [1] eine Hilfestellung zur Erstellung eines geeigneten Verfahrens veröffentlicht. Dort werden auch alle anderen Anforderungen an ein Backup (z. B. Wiederherstellbarkeit, Brandschutz, physische Absicherung) berücksichtigt.

1 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_3_Datensicherungskonzept_Edition_2021.pdf