SECURITY WHITE PAPER

für Backup und Ransomware Protection
mit der ANIO Backup Appliance for Veeam

08/2024 | Version 1.2

Unsere Services schaffen Ihnen freie Zeit.

ANIO

Impressum
ANIO Solutions GmbH
Währinger Straße 12/9, A – 1090 Wien
+43 1 5810 5820 | info@an.io | **an.io**

Text: Christian Buzanich
Fotos: Adobe Stock, shutterstock, canvas

INHALTSVERZEICHNIS

Unsere Services
schaffen Ihnen freie Zeit.

AN.IO

ANIO verschafft Ihnen Zeit, um sich auf Ihr Kerngeschäft zu fokussieren

ANIO ist mit 20 Jahren Erfahrung im Bereich Backup Ihr kompetenter Ansprechpartner, wenn es um Härtungsmaßnahmen und die Sicherheit Ihrer Daten geht, Verlässlichkeit und Sicherheit stehen dabei im Mittelpunkt. Unser Ziel ist es, mit einer End-to-End-Betreuung die Komplexität für unsere Kunden zu reduzieren, damit sie sich auf ihr Kerngeschäft konzentrieren können. Mit fertigen und vielfach getesteten Produkt-Paketen werden individuelle Backup-Anforderungen rasch analysiert und umgesetzt und bringen so für den Kunden Zeit- und Kostenersparnis.

Mit der Backup Appliance bietet ANIO eine moderne, umfassende und skalierbare Lösung, die Hard- und Software-Komponenten vereint und als zentrale Schnittstelle für alle Backup-Prozesse fungiert. Aufgrund der großen Anzahl an bei Kunden installierten Lösungen besteht eine höchstmögliche Zuverlässigkeit der Lösungen, die permanent weiterentwickelt und durch regelmäßige Updates und Patches sicher gehalten werden.

an.io

WAS IST RANSOMWARE?

Der Begriff Ransomware bezeichnet Schadprogramme, die den Zugriff auf Daten und Systeme einschränken bzw. unterbinden und für die Freigabe der Daten Lösegeld (englisch: ransom) verlangen. Das Schadprogramm kann auf zweierlei Arten fungieren: entweder es sperrt den kompletten Zugriff auf das System oder es verschlüsselt bestimmte oder gleich alle Daten. Eine solche Ransomware kann die Operation eines Unternehmens ver- bzw. behindern und damit großen Schaden anrichten.

Wie ist Ransomware entstanden?

Ransomware-Programme sind weder ein neues Virus noch eine moderne technologische Entwicklung. Die ersten Ransomware-Prototypen mit asymmetrischer Verschlüsselung wurden bereits in den 1990-ern entwickelt. Die sogenannte „Asymmetrie" bezeichnet die Tatsache, dass es bei der eingesetzten Kryptographie unterschiedliche Schlüssel zur Verschlüsselung sowie zur Entschlüsselung benötigt. Symmetrische Verschlüsselungsverfahren verwenden hingegen ein und denselben Schlüssel zur Ent- und Verschlüsselung. Die Verwendung von asymmetrischen Verschlüsselungsmethoden ermöglicht Ransomware, Daten auf einem System mit einem öffentlichen Schlüssel zu verschlüsseln, ohne den privaten freizugeben. Eine Entschlüsselung ohne den privaten Key ist mit dem jetzigen Stand der Technik nicht möglich.

Warum ist Ransomware erst jetzt ein Problem?

Als die ersten realisierbaren Ransomware-Konzepte mit asymmetrischer Kryptographie aufkamen, bestand noch ein organisatorisches Problem. Es war zwar möglich Daten zu verschlüsseln, jedoch verfügten die Cyberkriminellen über keine Möglichkeit ihre Opfer das Lösegeld bezahlen zu lassen, ohne dabei erwischt zu werden. Der Autor des „AIDS"-Trojaners versuchte beispielsweise Zahlungen an ein Postfach senden zu lassen, wurde jedoch daraufhin schnell verhaftet. Die Technologie der Ransomware gibt es also schon länger, jedoch war eine finanzielle Bereicherung mit viel Risiko verbunden. Das änderte sich schließlich als 2005 GPCode aufkam.

GPCode war ein simpler Trojaner, der zunächst alle Daten mit den Endungen .doc, .html, .jpg, .xls, .zip, und .rar verschlüsselte. Anschließend legte er im Verzeichnis, wo sich die Daten befanden eine Textdatei ab, die eine Zahlung verlangte. Die Bezahlung erfolgte dann über E-Gold, ein ehemaliges Bezahlungssystem, welches auf der karibischen Insel Nevis betrieben wurde und über Liberty Reserve (ein Unternehmen, das Bezahlungen mit virtuellen Währungen ermöglichte, die an Dollar oder Gold gekoppelt waren). Es gab mehrere Varianten von GPCode, jedoch hatten sie alle Mängel. Entweder verwendeten sie eine symmetrische Verschlüsselung oder sie löschten die Daten. Zudem waren damals noch hauptsächlich magnetische Festplatten im Einsatz, wodurch sich die Daten einfacher wiederherstellen ließen ohne Lösegeld zahlen zu müssen.

Cryptolocker kam schließlich im Septemper 2013 auf dem Markt. Es war die erste Generation der Ransomware, die Bitcoins für Zahlungen einsetzte. Das Aufkommen der Crypto Währung Bitcoin machte das Geschäftsmodell von Ransomware erst „sicherer" und damit lukrativ. So kam nach und nach ähnliche Schadsoftware auf. CryptDefense, TorrentLocker, CTB-Locker, CryptoWall, TeslaCrypt und AlphaCrypt, um ein paar zu nennen.

Zusammengefasst lässt sich also sagen, dass Ransomware erst mit der Kombination aus dem Geschäftsmodell mit digitaler Währung (Bitcoin, Monero etc.) zur Verbreitung und zu der heute bekannten digitalen Bedrohung geführt hat.

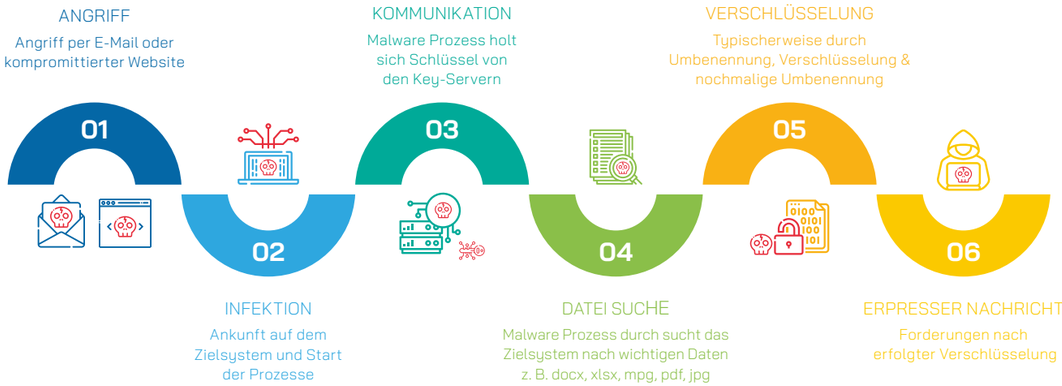
Was ist Ransomware-as-a-Service?

Ransomware as a Service (RaaS) ist ein Angebot von Schadsoftware, die gegen Bezahlung genutzt werden kann. Damit müssen Cyberkriminelle nicht mehr selbst über die technischen Fähigkeiten verfügen, um entsprechende Schadsoftware zu erstellen. Sie buchen die Erpressersoftware einfach als Dienst, um Unternehmen oder Privatpersonen anzugreifen.

RaaS hat seinen Aufschwung erlebt, als Ransomware Autor:innen eine Möglichkeit fanden die ganze Welt an ihrem Erfolg teilhaben zu lassen. Ende 2014 veröffentlichten Cyberkriminelle ein Ransomware-Toolkit mit Umsatzbeteiligungsmodel. Damit schufen sie ein lukratives, automatisiertes Geschäftsmodell, das viral gewachsen ist. Es ist sehr einfach daran teilzunehmen und die finanzielle Belohnung ist sehr hoch. Die meisten Modelle sehen eine Aufteilung des Ertrags (meist in Bitcoin) oft bei 70/30 zugunsten des Partners auf. Der Partner benötigt keine besonderen Prorammierkenntnisse, sondern „nur" die Bereitschaft die Ransomware zu verbreiten.

Was ist eine automatisierte Ransomware-Attacke?

Eine automatisierte Ransomware-Attacke zielt auf die Menge ab, das heißt: so viele Systeme wie möglich infizieren und dabei kleinere Lösegelder verlangen. Die meisten automatisierten Ransomware-Attacken werden über generische Phishingmails oder angreifbare Systeme eingeschleust (remote code execution). Die verlangten Lösegelder bewegen sich dabei zwischen 100 € und 2.000 €. WannaCry ist wohl die bekannteste Ransomware aus diesem Bereich. Da diese Art von Attacken immer weniger lukrativ werden, geht der Trend in den letzten Jahren zu gezielten Angriffen.



Ransomware Infektion

Was ist eine gezielte Ransomware-Attacke?

Anfang 2019 starteten die ersten gezielten Attacken. Bei diesen Angriffen wird nicht großflächig infiziert, sondern er werden gezielt Unternehmen ausgewählt und angegriffen. Die verlangten Lösegelder dabei mehreren Millionen betragen und oft sind die Forderungen an die Umsätze der Opfer gekoppelt.

Dabei investieren die Angreifer Wochen oder Monate, um sich Zugang zu ausgewählten Systemen zu verschaffen und möglichst viele Daten zu verschlüsseln. Durch die fortschreitende Digitalisierung der Unternehmen ist diese Art von Attacken deutlich lukrativer geworden und die Anzahl solcher Angriffe ist enorm gewachsen.

Gezielte Ransomware-Attacke

– 4 %

Die Zahl der Malware-Angriffe ist 2021 insgesamt nur 4 % gesunken – eine Trendumkehr seit dem 22-prozentigen Rückgang zum Halbjahr.

https://www.sonicwall.com/de-de/2022-cyber-threat-report/

WIE FUNKTIONIERT EINE RANSOMWARE-ATTACKE?

Ransomware geht grundsätzlich in sechs Schritten vor, um sein Ziel zu erreichen.

01 Die Verteilung

Ransomware wird durch Phishing-Schemata, E-Mail-Anhängen oder Downloads verteilt und durch Website-Kompromittierungen auf einem Endpunkt installiert. Trotz Unternehmensschulungen und Medienberichten sind dabei Benutzer:innen das schwächste Glied.

02 Die Infektion

Die Binärdatei oder das Office Dokument mit Makros kommt auf dem Computer der/der Benutzer:in an uns startet die Prozesse, um seinen Zweck zu erfüllen.

Beispielweise könnte die Ransomware folgendes tun:

a. eine eindeutige Computerkennung generieren
b. im Hintergrund die Binärdatei herunterladen.
c. sicherstellen, dass sie einen Neustart überlebt, indem sie das Programm so installiert, dass es beim Neustart ausgeführt wird. (Autostart)
d. Schattenkopien, Startreparatur und Windows-Fehlerbehebungen deaktivieren.
e. das Windows Security Center, den Windows Defender, den Windows Update Service, „Error Reporting" und BITS stoppen.
f. Sich an explorer.exe und svchost.exe hängen.
g. die externe IP-Adresse abrufen.
h. Weiter zu Schritt 3

03 Die Kommunikation

Der Ransomware-Prozess holt sich die „Public-Keys" von einem oder mehreren Kontrollservern im Internet. Diese braucht es, um die Daten asymmetrisch zu verschlüsseln. Der gesamte Datenverkehr zum Kontrollserver wird mit dem AES Verschlüsselungs-algorithmus verschlüsselt.

04 Die Dateisuche

Der Ransomware-Prozess sucht systematisch nach Dateien im System. Es verwendet einen Algorithmus, um zu erkennen welche Dateien wichtig sein könnten. Beispielweise sind das Dateien mit den Endungen jpg, docx, xlsx, pptx, pdf sqlite, .catproduct, .rdp, .accdb, .catpart, catdrawing, .3ds, .dwt und .dx

05 Die Verschlüsselung

Der fünfte Schritt ist die Verschlüsselung. Hier werden etwa die Daten zuerst verschoben, dann unbenannt und schließlich verschlüsselt. Nach der erfolgreichen Verschlüsselung werden die Daten nochmals unbenannt.

06 Die Erpresser-Nachricht/ Lösegeldforderung

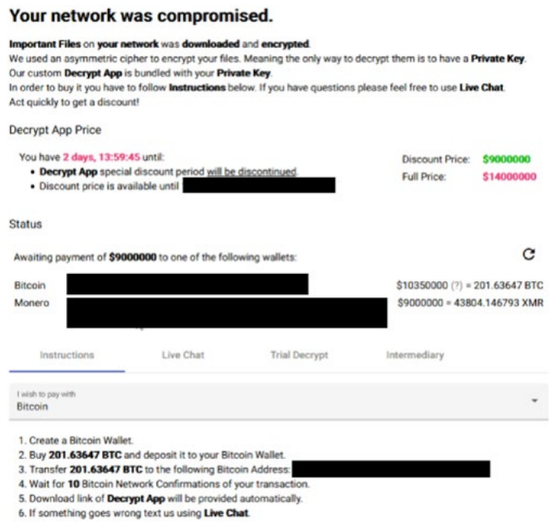
Der letzte Schritt ist die Lösegeldforderung, typischer-weise durch die Übernahme des Bildschirms des infizierten Endpunkts und einer Forderung nach Zahlung.

An diesem Punkt hat der/der Benutzer:in grundsätzlich keine andere Wahl, als das Lösegeld zu zahlen und auf die Lieferung eines verwendbaren Schlüssels zum Entsperren der Dateien zu hoffen.

Einzige Ausnahme: man hat eine gehärtete Backup-Lösung, um die Dateien wiederherzustellen!


```
->> Introduction

Important files on your system was ENCRYPTED and now they have have "wpzlbji"
extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your system was DOWNLOADED and it will be PUBLISHED if you refuse to
cooperate.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank
statements.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...

>> CAUTION

DO NOT MODIFY FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY.

>> Recovery procedure

Follow these simple steps to get in touch and recover your data:
1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to:
http://2cuqgeerjdba2rhdiviezodpu3lc4qz2zjf4qin6f7std2evleqlzjid.onion/?(ACCESS_KEY)
```

Beispiel Lösegeldforderung



Beispielseite für BlackCat Ransomware

Organisatorisch

Ausfall der Einnahmen

Ein Ransomware-Angriff kann die Betriebsfähigkeit einer Organisation stark beeinträchtigen. Selbst wenn die Organisation gut vorbereitet ist und über funktionsfähige Backups verfügt, kann die Wiederherstellung betroffener Systeme Stunden dauern. Schlimmer noch, Organisationen, die nicht so gut vorbereitet waren oder deren Backups möglicherweise während des Angriffs kompromittiert wurden, könnten Tage oder Wochen brauchen, um wieder die volle Betriebskapazität zu erreichen. Das bedeutet, dass ihre Einnahmen zurückgehen oder ganz eingestellt werden, während sie die Daten wiederherstellen.

Reputationsschaden und Opportunitätskosten

Eine Datenschutzverletzung oder ein Ransomware-Angriff kann den Ruf eines Unternehmens beeinträchtigen. Einige Kunden sehen einen erfolgreichen Angriff möglicherweise als Hinweis auf schwache Sicherheitspraktiken oder sind von einer Dienstunterbrechung so stark betroffen, dass sie sich entscheiden, ihre Geschäfte woanders zu tätigen.

Finanzieller Schaden

Ransomware verursacht unerwartete Kosten und kann sehr teuer werden. Zusätzlich zu den Einnahmeverlusten, die eine Organisation erleiden kann, gibt es weitere Kosten, die auf das betroffene Unternehmen zukommen. Zu den offensichtlicheren Kosten gehören: die Kosten für die Lösegeldzahlung (falls bezahlt); die Kosten für die Behebung des Vorfalls, einschließlich neuer Hardware, Software und Forensikdienste; Versicherungsselbstbehalte; Anwaltsgebühren und Rechtsstreitigkeiten; und Öffentlichkeitsarbeit. Andere, weniger offensichtliche Kosten können sein: Versicherungsprämienerhöhungen; Abwertung der Reputation und/oder der Marke; und Verlust von geistigem Eigentum.

Datenverlust

Während eines Ransomware-Angriffs verschlüsselt ein böswilliger Akteur zahlreiche Dateien, wodurch die Dateien und häufig die darauf angewiesenen Systeme unbrauchbar werden. Wenn kein Lösegeld gezahlt wird, werden diese verschlüsselten Dateien dauerhaft gesperrt, sodass die Organisation die Informationen nach Möglichkeit neu generieren muss. Doch selbst wenn ein Lösegeld gezahlt wird, gibt es keine Garantie dafür, dass der/die Angreifer:in wohlwollend handelt und einen Entschlüsselungsschlüssel bereitstellt. Darüber hinaus ist es auch bei Bereitstellung eines Schlüssels möglich, dass der Ransomware-Angriff erhebliche zerstörerische Schäden verursacht hat, die ohnehin einen Wiederaufbau der betroffenen Systeme erfordern können. Wenn ein/e Angreifer:in außerdem ein Geschäftsgeheimnis, geschützte Informationen oder personenbezogene Daten (PII) gestohlen hat, könnte der Verlust dieser Daten rechtliche Schritte nach sich ziehen oder zum Verlust eines Wettbewerbsvorteils führen.

Technische Auswirkungen

Betroffene Systeme und Arten der Angriffe bei den uns bekannten Fällen waren sehr unterschiedlicher Natur. Hier eine kurze Auflistung der von uns bei Einsätzen gesehenen Varianten und betroffenen Produkten, welche im Zuge einer Attacke betroffen waren.

- VMware: auf Basis Ebene wurden Guest vmdks verschlüsselt und vmx Dateien gelöscht
- Windows Server Systeme aller Art, wie z. B. Domain Controller, SAP Systeme, Exchange, Fileserver, uvw.
- Steuerungs- und Produktionsanlagen waren betroffen. Im Detail die Steuerungsserver von Maschinen oder medizinischen Geräten
- Auf NAS Systeme wurden Snapshots gelöscht oder Replikatinsketten unterbrochen
- Backup Appliances diverser Hersteller
- Backup Software jeglicher Art wie z. B. IBM Spectrum Protect, Veeam, Dell Avamar, Veritas NetBackup, Commvault

Backupsyteme wurden über verschiedenste Methoden sabotiert:

- Über die Backup API/Schnittstellen
- Zerstörung über die Management Zugänge auf Backup Server, Media Agent/Server oder Appliances
- Verschlüsselung bei Windows Systemen
- Zerstörung über Hardware Management Interfaces der zugehörigen Storage-/Server Systeme

↑ 6 %
= 60,1 Mio.

IoT-Malware

Die Zahl stieg 2021 um 6 % weltweit auf insgesamt 60,1 Millionen zum Jahresende

https://www.sonicwall.com/de-de/2022-cyber-threat-report/

WO LIEGEN DIE ANGRIFFSFLÄCHEN EINER ORGANISATION?

Mitarbeiter:innen

Die einfachsten und erfolgreichsten Hack-Angriffe sind durch das Ausnutzen der Naivität und mangelnder Kenntnisse der Anwender:innen möglich. Daher gelten unwissende bzw. ungeschulte Mitarbeiter:innen in der Cybersecurity als das schwächste Glied eines Unternehmens. Das Öffnen eines Links oder einer Datei, das Anstecken eines USB-Sticks genügen, um einen Ransomware-Verschlüsselungsprozess zu starten.

Phishing Mails

Bei einer Phishing Mail-Attacke senden die Angreifer:innen Emails an Mitarbeiter:innen und verleiten sie einen Link oder eine Datei zu öffnen. Der Absender gibt sich oft als offizielle Behörde, Bank oder IT-Mitarbeiter aus. Es werden für die Opfer sorgsam angepasste E-Mails verschickt, um die Klick-Wahrscheinlichkeit zu erhöhen. Die Öffnungsrate ist besonders hoch, wenn das Unternehmen seinen Mailserver nicht richtig abgesichert hat, wodurch sich Kriminelle als ein/e Kollege:in oder als Vorgesetzte/r ausgeben können und in deren Namen E-Mails an die Opfer verschicken (Mail Spoofing).

USB-Sticks

Bei einem USB-Stick-Angriff schleusen Cyber-Kriminelle USB-Sticks in das Büro-Gebäude. Wenn einer der Sticks an ein Gerät angesteckt wird, führt dieser eine Schadsoftware aus. Entweder starten dann automatisch Tastatur Eingaben (HID Spoofing), oder der Datenträger beinhaltet MS-Office Dateien, die beim Öffnen Makros Schadcode ausführen.

Physischer Angriff

Bei einem physischen Angriff verkleiden sich Angreifer:innen und geben sich als Mitarbeiter:innen oder z. B. als Reinigungskraft aus, um sich Zugang zu Büroräumen zu verschaffen. Sobald das gelingt, können die Angreifer:innen über mehrere Wege Schaden anrichten. Etwa durch Installieren von Schadsoftware auf Firmengeräten, indem sie Keylogger platzieren und damit alle Tastatureingaben mitlesen oder durch das Platzieren von Hardware im Firmennetzwerk über die sie Angriffe ausführen können.

Angriffe auf verwundbare Systeme (Exploits)

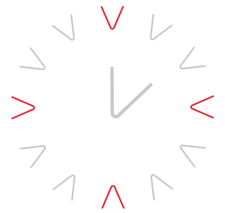
Zahlreiche Unternehmen haben aufgrund von mangelndem Know-How oder Fachkräftemagel ihr Schwachstellen- und Patch-Management nicht im Griff. Für Cyberkriminelle sind derartige Schwachstellen eine leichte Beute. Meist reicht eine einzige Schwachstelle aus, um Schadsoftware einzuschleusen. Einer Studie des Cyber-Sicherheitsunternehmens SenseCy aus dem Jahr 2020 zufolge wurden bei 180 untersuchten Sicherheitsvorfällen lediglich vier Schwachstellen ausgenutzt.

Remote Desktop Protokoll und Home Office

Während der COVID-19 Pandemie wurden viele Remote Desktop Protokoll (RDP) Server über das Internet eingerichtet, um Mitarbeiter:innen so schnell wie möglich das Arbeiten von zuhause zu ermöglichen. Dabei wurde oft die Sicherheit vernachlässigt. Angriffe mit Credential-Stuffing- oder Brute-Force-Methoden gegen internetexponierte RDP- und VPN-Dienste sind dadurch sehr häufig geworden. Die Angriffe zielen darauf ab, durch das systematische Erraten, die Verwendung von Kennwortlisten oder zuvor erbeuteter Anmeldedaten die Authentifizierung für den Zugriff auf Firmen-Geräte oder -Dienste zu erlangen.

Angriffsfläche Backup

Backups sind die effektivste Lösung, um Unternehmensdaten vor Datenverlust durch Ausfälle von Systemen wegen schadhafter Hardware, menschlichem Versagen oder auch einer Ransomware-Attacke zu schützen. Da Ransomware im letzten Jahrzehnt zu einem der Hauptprobleme geworden ist, werden Backups immer öfter effektiv zur Wiederherstellung einer durch Ransomware zerstörten IT-Infrastruktur eingesetzt. Die Cyber-Kriminellen sehen hierbei nicht untätig zu. Um das Fortlaufen ihres Geschäftsmodells zu gewährleisten, sind Backup-Systeme neuerdings mitunter eines der wichtigsten Ziele der Angreifer:innen im Rahmen gezielter Attacken.



Backup Server

Um das Management der Backups zu vereinfachen, sind die Backup-Systeme meist ein Teil der bestehenden IT-Infrastruktur. Das bedeutet, dass sie dasselbe Authentifizierungs-System und dieselben Storage-Komponenten nutzen, wie die restliche IT. Durch gezielte und langgeplante Angriffe erlangen die Hacker:innen in den meisten Fällen administrative Rechte, etwa durch die Übernahme oder Neuerstellung entsprechender Accounts. Sind die Backup-Systeme Teil des Active Directories, haben die Angreifer:innen damit auch vollen Zugriff auf alle Backups. Unter Umständen sind auf dem Backup-Systemen oft noch mehr Daten aus sensiblen Unternehmensbereichen wie z. B. der Personalabteilung oder Forschung und Entwicklung gespeichert, auf die die Angreifer:innen vielleicht noch gar keinen Zugriff hatten.

Virtualisierungssysteme

Die Virtualisierungstechnologie ermöglicht es den Unternehmen ihre IT-Systeme effektiv zu nutzen und so eine komplexe IT-Infrastruktur mit stark reduzierten Kosten zu betreiben. Die gebotenen Features wie Templates, Snap-Shots und diverse Restore-Funktionen helfen, nach einem Ausfall, schnell wieder den Normalbetrieb zu erreichen. Ähnlich wie bei einem Backup-Systemen hilft dies den Unternehmen, ohne Zahlung eines Lösegelds wieder operativ tätig zu werden. In die letzten Jahre haben sich aber auch die entdeckten Schwachstellen diverser Virtualisierungssysteme gehäuft. Da die Virtualisierungssysteme aber zum Beheben dieser Schwachstellen zum Teil mehrfach neu gestartet werden müssen, bedeutet dies auch, dass alle virtuellen Systeme abgeschaltet werden müssen und dass die Wartung sehr genau geplant werden muss. Oft bleibt keine Zeit, um ein entsprechendes Wartungsfenster einzurichten und die nötigen Arbeiten durchzuführen. Genau diesen Umstand nutzen die Angreifer:innen aus und greifen seit geraumer Zeit gezielt Virtualisierungssysteme an. Inzwischen gibt es Schadsoftware, die diese Angriffe vollautomatisiert im Zuge eines Ransomware-Angriffs durchführen kann. Besonders kritisch ist es, wenn auch die Backup-Systeme virtualisiert sind. Oft ist die Authentifizierung der Virtualisierungssysteme auch an das Active Directory angebunden. Haben die Angreifer:innen bereits administrative Rechte erlangt, haben sie auch volle Handhabe über diese Systeme.

Storage

Die exponentiell wachsenden Datenmengen stellen die Unternehmen immer wieder vor die Herausforderung der Speicherung. So ist irgendwann der Punkt erreicht, an dem ein Unternehmen an einem Storage System nicht mehr vorbeikommt. Oft werden fertige Network Attached Storage (NAS) Systeme gekauft. Diese bieten zwar ein gutes Preis-Leistungs-Verhältnis, sind aber sehr leicht angreifbar. Sie weisen leider oft kritische Schwachstellen oder administrative Fehlerkonfigurationen auf, wodurch ohne Authentifizierung ein lesender und schreibender Zugriff auf die Netzwerklaufwerke des NAS ermöglicht wird. Sollten doch alle Zugriffe auf das Storage eine Authentifizierung erfordern, wird dies oft auch über das Active Directory geregelt. Damit ergibt sich das Problem, dass sobald Angreifer:innen administrative Rechte erlangt haben, sie auch vollen Zugriff auf alle Daten haben und diese verschlüsseln können.

WELCHE VERTEIDIGUNS-STRATEGIEN GIBT ES?

Mitarbeiter:innen auf Cybersicherheit sensibilisieren

Die größte Bedrohung stellen die Mitarbeiter:innen da, die unwissentlich Ransomware installieren. Der häufigste Entry Point von Ransomware kann auf das Fehlverhalten der Mitarbeiter:innen zurückgeführt werden. Die Belegschaft regelmäßig zu schulen und zu sensibilisieren, ist daher essenziell.

Endpoint Protection

Neben der Sensibilisierung der Belegschaft ist die effektivste Methode zum Schutz vor Ransomware-Angriffen die Nutzung von verhaltensbasierten Virenschutzprogrammen und Webfiltern. Sie hindern Ransomware daran ein Gerät im Netzwerk zu erreichen bzw. erkennen schadhaftes Verhalten.

Updates

Viele Cyberkriminelle nutzen Schwachstellen in veralteten Systemen aus, um Geräte im Netzwerk zu infizieren. Installieren Sie immer die neuesten Updates und Patches, um die Angriffsflächen zu minimieren, da diese die neuesten Verbesserungen und Korrekturen beinhalten.

Spam-Filter und Web-Gateway-Filter

Spam-Filter und Web-Gateway-Filter zielen darauf an, Ransomware daran zu hindern überhaupt ein Gerät über Phishing-Mails und IPs zu erreichen. Der Einsatz dieser Filter wird daher stark empfohlen.

Anwendungskontrolle und Whitelisting

Anwendungskontrolle und Whitelisting ist eine effektive Methode, in der das Ausführen von nur bekannten Anwendungen auf Firmengeräten erlaubt wird. Damit wird gewährleistet, dass unbekannte EXE oder DDL Dateien nicht auf Firmengeräten installiert werden können. Das reduziert das Risiko von Ransomware-Angriffen drastisch. Jedoch ist dies ein äußerst aufwendiges Vorhaben.

Ressourcen für unbekannte Prozesse limitieren

Mithilfe von „Host Intrusion Prevention" lassen sich Ressourcen für unbekannte Prozesse limitieren, wodurch auch das Risiko von Ransomware-Attacken effektiv geschränkt wird.

Makros deaktivieren

Auf MS Office Dokumenten sollten Makros grundsätzlich deaktiviert sein. Nur wer sich bei den Makros sicher ist, sollte ihre Ausführung erlauben. MS Office Makros sind eine effiziente Methode für Ransomware, Computer zu infizieren. Daher bedarf es genaueste Prüfung viel Vorsicht, bei der Aufforderung eines Dokuments zur Aktivierung der Makros. Im Zweifelsfall nicht aktivieren.

Kein Admin, wenn es nicht sein muss

Das Credo lautet: so wenige Rechte wie möglich, so viele wie notwendig. Wer nur im Internet surft oder an Dokumenten arbeitet, muss dies nicht als Administrator machen. Als Admin eingeloggt zu sein, ist sehr gefährlich da eine Ransomware-Infektion eines Admin-Accounts erheblichen Schaden anrichten kann. Außerdem sollten SSH Verbindung als „root" deaktiviert werden und Admin-Rechte erst dann vergeben werden, wenn sie benötigt werden.

Zugriffsregeln bei Anwendungen beschränken

Es sollten Zugriffskontrollregeln für gezielte Datenerweiterungen geschrieben werden. Damit sollen nur erlaubte Anwendungen auf Daten zugreifen oder verändern dürfen. Außerdem soll verhindert werden, dass „nicht genehmigte" Prozesse Dateien ändern. Diese lassen sich blockieren, indem Regeln für Host Intrusion Prevention-Systeme oder Zugriffsschutz geschrieben werden.

Sandboxing für verdächtige Prozesse

Wenn ein Prozess als verdächtig eingestuft wird, sollte dieser in Quarantäne kommen und zur Untersuchung in einer Sandbox landen. Ziel ist dabei, dass Verdächtiges auf einem System untersucht wird, auf dem es keinen Schaden anrichten kann.

Firewall Regeln

Firewall Regeln können bekannte bösartige Domains und IP-Adressen blockieren. Das ist eine Standard-Funktion jeder Firewall und ein Must-Have.

Tor Verbindungen deaktivieren

Tor ist ein anonymes Internet-Kommunikationssystem, das auf einem verteilten Netzwerk basiert. Tor wird von Ransomware verwendet, um die Kommunikation mit Kontrollservern zu verschleiern.

Bei Unternehmen, die diese Technologie für ihre Zwecke nicht benötigen, sollten Administratoren erwägen, den Zugriff auf diese Netzwerke zu blockieren. Oft funktioniert Ransomware nicht, wenn sie keine Verbindung zu ihrem Server aufbauen kann.

Proxy-/Gateway-Scanner-Signaturen

Für diejenigen mit Proxy- und Gateway-Appliances: diese Technologien können so konfiguriert werden, dass sie nach bekanntem Ransomware-Kontrollserver-Datenverkehr scannen und ihn blockieren. Die meisten Ransomware-Programme können den Betrieb nicht fortsetzen, wenn sie den für die asymmetrische Verschlüsselung erforderlichen öffentlichen Verschlüsselungsschlüssel nicht abrufen können.

Backups

Regelmäßige Backups helfen dabei Daten wiederherzustellen, wenn sie verschlüsselt wurden. Backups erlauben es mit der Wiederherstellung in der Zeit zurückzugehen, bis zu einem Zeitpunkt, bevor das System mit Ransomware infiziert wurde und diesen Zustand wiederherzustellen.

Zugriff auf Shares beschränken

Viele Ransomware-Varianten suchen nach Zugriff auf Dateien auf anderen Systemen– wie Dateiservern, zusätzlichen Volumes usw. – und verschlüsseln alles, was sie finden können, um maximalen Schaden anzurichten. Es ist eine Erwägung wert, die auf freigegebenen Volumes zulässigen Operationen einzuschränken.

3-2-1 Backup

Das ideale Backup besteht aus drei Datenkopien, davon zwei Medien und ein externes „Air-Gapped" Backup, das nicht mit dem Computer verbunden ist. Bei einem „Air-Gapped" Backup kann eine Ransomware das Speichermedium nicht erreichen und somit auch nicht beschädigen. Mit einem Angriff ist leider immer zu rechnen. Daher sind solide Backups da A und O, um Daten wiederherzustellen.

Unsere Services
schaffen Ihnen freie Zeit.

ANIO BACKUP SOLUTION

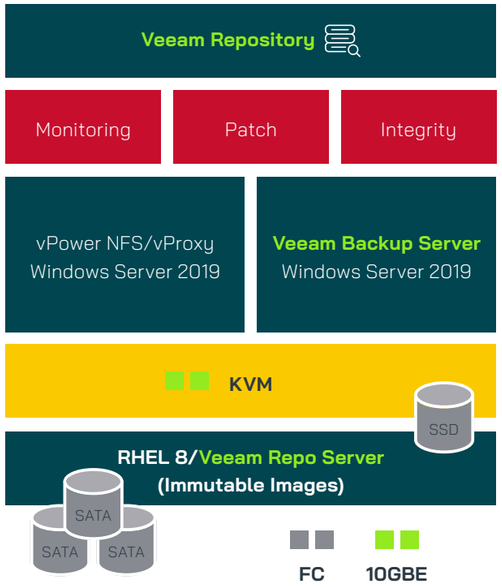
ANIO
BACKUP SOLUTION

Die ANIO Backup Appliances helfen Kunden dabei, bekannte Verteidigungsstrategien wirksam und effizient auch in deren Backup Umgebung nutzbar zu machen.

Die Lösung besteht aus mehreren Komponenten. Der Unterbau ist immer ein von ANIO betreutes und gewartetes Linux Betriebssystem auf Basis Red Hat Enterprise Linux mit Langzeitsupport. In der Veeam-Variante unserer Appliances werden auf Basis KVM die notwendigen Veeam-Rollen als Guest unter Windows betrieben.

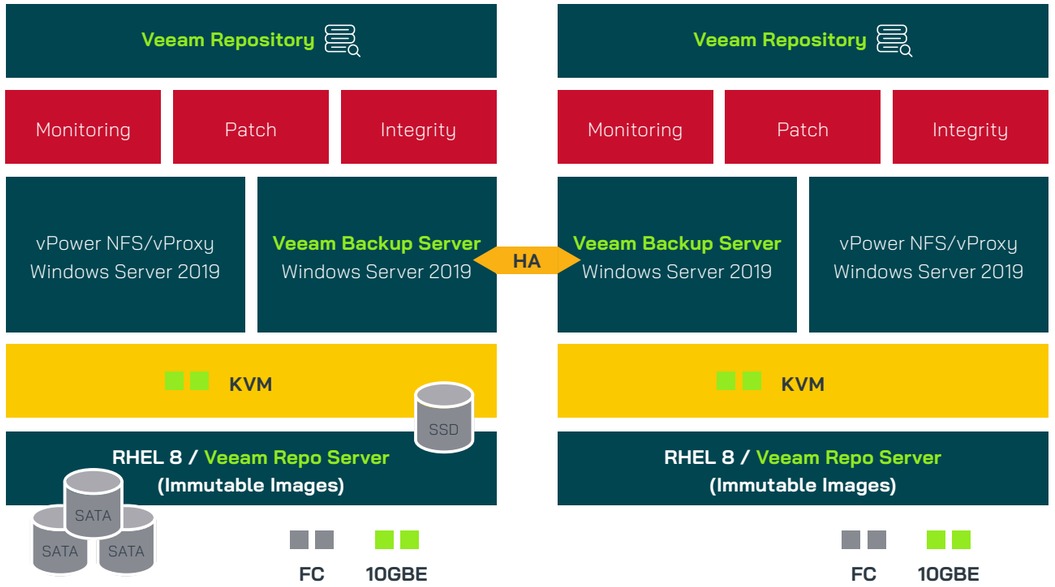
Je nach Variante kann die Appliance auch eine Veeam VBR Rolle inkludieren – auch als HA-Lösung mit zwei Appliances verfügbar. Diese beiden Varianten sind nicht Teil des Standardumfangs, können aber als optionale Implementierung umgesetzt werden.

ANIO Veeam Backup Appliance – Standalone



Schemata ANIO Veeam Backup Appliance – Standalone

ANIO Veeam Backup Appliance HA



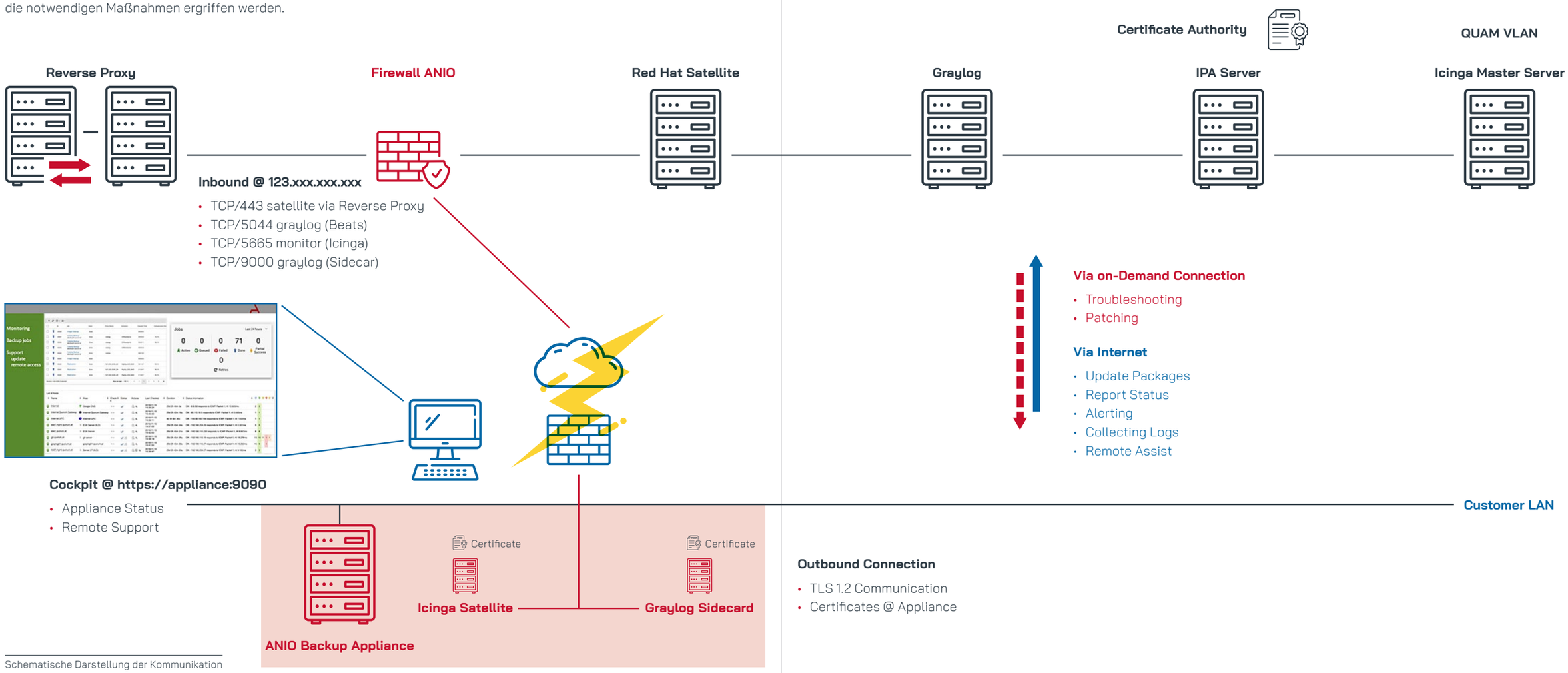
Schemata ANIO Veeam Backup Appliance HA

AKTIVES LOGGING UND MONITORING

Die ANIO Backup Appliances werden aktiv auf der Hardware- und Software Ebene überwacht. ANIO betreibt aktives Log Monitoring der iDRAC Management Interfaces, um frühzeitig auf Hardware-Probleme hinzuweisen. Alle von ANIO betriebenen Services sind Teil des Log Managements. Zusätzlich zu den Betriebssystem-Logs kommt SE-Linux im Permissive Mode zum Einsatz.

Dadurch verfügen alle ANIO Backup Appliances über ein vollständiges zentrales Log-Management. Dies ermöglicht es in Echtzeit auf Probleme zu reagieren. Mithilfe der gesammelten Logs kann damit nachvollzogen werden, was passiert ist und dementsprechend die notwendigen Maßnahmen ergriffen werden.

Kurzum, ANIO erkennt in Echtzeit Probleme oder Angriffsversuche bei den Backups seiner Kunden.



Schematische Darstellung der Kommunikation

Welche Technologien werden verwendet?

Verwendet wird Graylog Enterprise als zentrales Logmanagement zur Sammlung und Auswertung der Appliance Daten. Die Daten werden verschlüsselt an unsere Managementdomäne übermittelt.
Der Graylogserver ist nur über Port 9000 und 5044 erreichbar.

Wie lange werden die Logs gespeichert?

Die Logs werden für 12 Monate aufbewahrt und stehen für weitere Analysen zur Verfügung. Nach Ablauf der Wartung oder Dekommisionierung der Server werden diese Daten gelöscht.

Was ist im zentralen Logging drinnen? Was wird überwacht?

Die an uns gesendeten Logs beinhalten die Informationen aus dem Systemlogs der Linux Installation.

- /var/log/*.log
- /var/log/cron
- /var/log/dmesg
- /var/log/firewalld
- /var/log/maillog
- /var/log/messages
- /var/log/secure
- /var/log/icinga2/*.log
- /var/log/audit/audit.log

Windows Logs:

- Application
- System
- Security

Mit icinga (Monitoring Software) werden folgende Checks durchgeführt:

CPU	Prüft den Hardwarestatus der Komponente
Fans	Prüft den Hardwarestatus der Komponente
Temperatures	Prüft den Hardwarestatus der Komponente
Memory	Prüft den Hardwarestatus der Komponente
Power Supplies	Prüft den Hardwarestatus der Komponente
Power Consumption	Prüft den Hardwarestatus der Komponente
Voltages	Prüft den Hardwarestatus der Komponente
Batteries	Prüft den Hardwarestatus der Komponente
RAID Controller HW	Prüft den Hardwarestatus der Komponente
RAID Volumes	Prüft den Hardwarestatus der Komponente
Physical Disks	Prüft den Hardwarestatus der Komponente
Betriebssystem Checks (inkl. KVM)	
CPU Load	Prüft die Auslastung der CPU
Memory Usage	Prüft die Auslastung des Speichers
Filesystem Usage	Prüft die Auslastung der Filesysteme
SWAP Usage	Prüft die Auslastung der Auslagerung
PING	Prüft die Funktion des Netzwerks
Weitere Veeam spezifische Checks optional	Weitere Veeam spezifische Checks optional

Patch Management

ANIO übernimmt sowohl die Wartung, das Patching und auch das Vulnerability Management der Backup Appliance auf der Software- und Hardware Ebene.
Kurze und regelmäßige Patch-Intervalle werden über den Red Hat Satellite Server abgewickelt, um die Systeme immer am aktuellen Stand zu halten.
Als Dell Titanium Partner hat ANIO den Support der verwendeten Hardware immer im Blick. ANIO verwaltet die nötigen Firmware Updates als auch den Tausch von Komponenten.

Was ist der Red Hat Satellite Server? Wie werden Patches/ Updates gemacht?

Der ANIO Satellite Server ermöglicht ein geordnetes Updaten von Red Hat Linux Betriebssystemen durch die Content View Funktionalität. Diese Content Views ermöglichen individuelle Repositories aus den RedHat Repos zu erstellen, und somit eine Abbildung eines Releasestands unabhängig von Upstreamänderungen zu generieren. Diese Content Views werden vor dem Update von ANIO intern überprüft und gegebenfalls angepasst, um diese so entstehenden Updates im Einklang mit der IT Abteilung des Kunden auszurollen.

In welchen Intervallen wird upgedated? Wie lange ist die Downtime beim Patching?

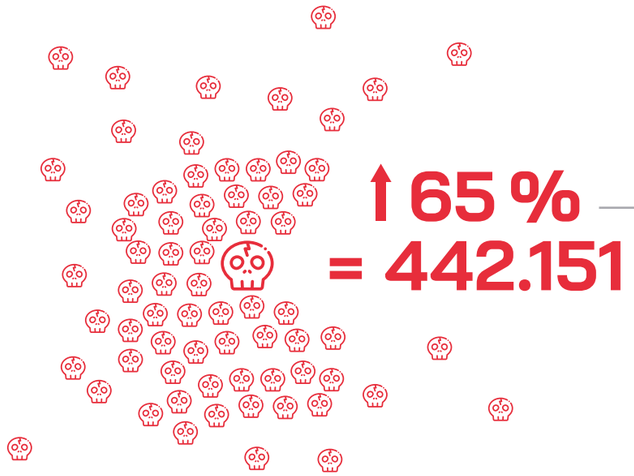
Security Updates werden zeitnahe ausgerollt. Reguläre Updates der verwendeten RHEL 8 Version halbjährlich. Diese Updates erfordern in der Regel keine Downtime. Ausnahmen werden kommuniziert und infolge mit dem Kunden abgesprochen.

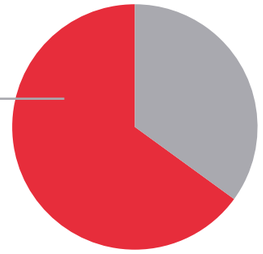
Werden Vulnerability Checks gemacht? Wenn ja, wie oft?

Vulnerability Checks sind ebenfalls Teil unserer Dienstleistung und werden durch externe Dienstleister einmal jährlich auf auf einer eigens dafür abgestellten Appliance mit dem Basisimage durchgeführt. Die Ergebnisse werden nach Rücksprache mit unseren Kunden auf die schon in Betrieb bestehenden Appliances ausgerollt. Das Ergebnis solcher Checks ist auf Anfrage für bestehende Kunden erhältlich. Ebenfalls werden unsere Kunden proaktiv informiert, wenn neue Exploits bekannt werden die für die Appliances relevant sind und was der Impact bzw. Gegenmaßnahmen sind.

Welche Firewall Einstellungen werden benötigt?

Auf den ANIO Backup Appliances sind nur die unbedingt nötigen TCP/IP Ports geöffnet. Jede andere Verbindung wird von der integrierten Firewall blockiert. Damit wird die Angriffsfläche auf ein Minimum reduziert.





Die RTDMI™-Technologie identifizierte 442.151 brandneue Varianten im Jahr 2021; eine Zunahme um 65 %.

https://www.sonicwall.com/de-de/2022-cyber-threat-report/

Welche Ports sind offen und warum? Ist die Kommunikation verschlüsselt? Wie wird eine sichere Kommunikation gewährleistet?

Eingehend erlaubt sind die Ports 22 (SSH) und die von NetBackup benötigten Ports. Das Cockpit (9090) und das Icinga Webinterface (9443) sind bei Auslieferung standardmässig deaktiviert. Jede dieser Kommunikation ist verschlüsselt.

Die ausgehende Kommunikation wird in Rücksprache mit dem Kunden individuell angepasst. Die Kommunikation mit der ANIO Managementumgebung muss gewährleistet sein. Die für Veeam spezifischen Ports werden ebenfalls aktiviert.

Source	Target	Protocol	Port(s)	Notes
Backup Server	Backup Repository (Linux)	TCP	22	Port use as control channel from the console to the target Linux host.
Backup Server	Backup Repository (Linux)	TCP	2500 – 3300	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigend.
Backup Repository (Linux)	Backup Server	TCP	2500 – 3300	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigend.
Backup Proxy	Backup Repository (Linux)	TCP	22	Port use as control channel from the console to the target Linux host.
Backup Proxy	Backup Repository (Linux)	TCP	2500 – 3300	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigend.
Backup Repository (Linux)	Backup Proxy	TCP	2500 – 3300	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigend.
Backup Repository (Windows)	Backup Repository (Windows)	TCP	2500 – 3300	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigend.
Backup Repository (Windows)	Backup Repository (Linux)	TCP	2500 – 3300	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigend.
Backup Repository (Linux)	Backup Repository (Windows)	TCP	2500 – 3300	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigend.
Backup Repository (Linux)	Backup Repository (Linux)	TCP	2500 – 3300	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigend.

Gibt es eine Angriffsfläche über Active Directory?

Keine Angriffsfläche über Active Directory

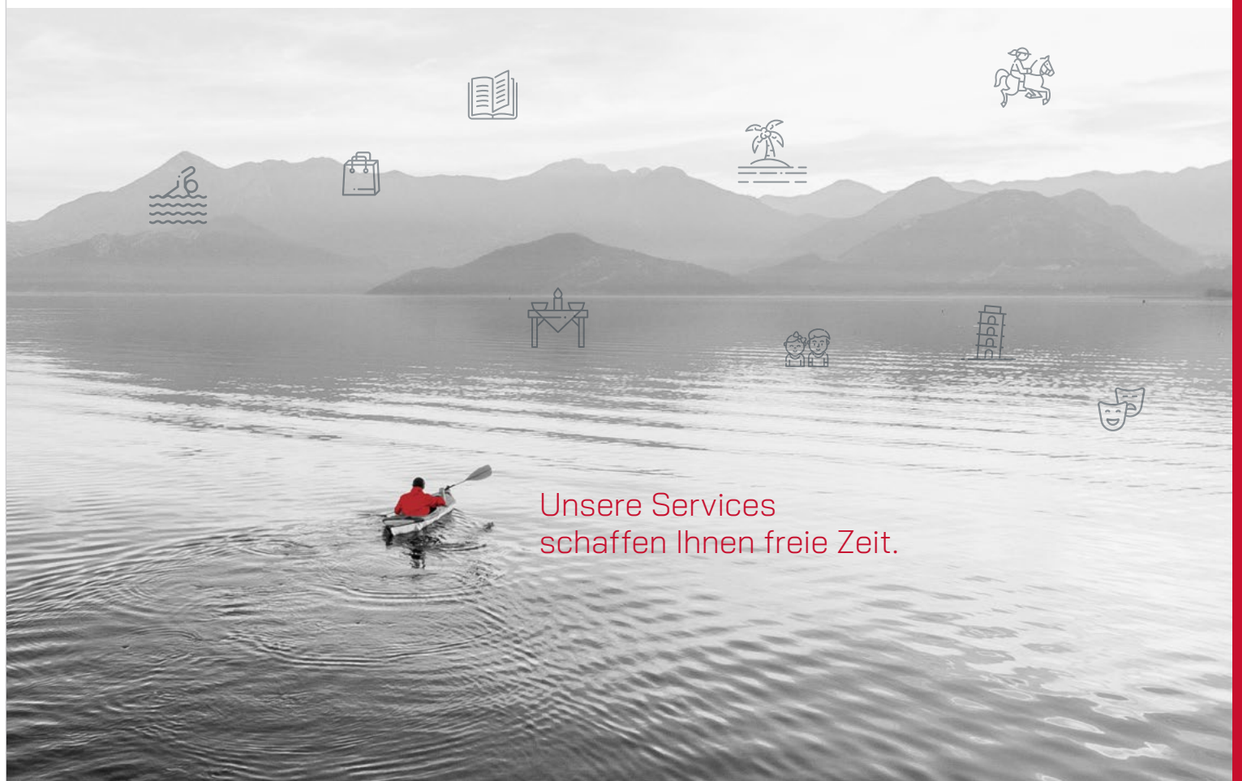
Unsere Lösungen werden nicht ins Active Directory eingebunden, was sie immun gegen Architektur- oder Konfigurationsfehler der Active Directory Authentifizierungs-Dienste NTLM und Kerberos macht.

Welches Authentifizierungssysteme werden verwendet?

Der Linux Server basiert auf PAM mit den notwendigen Modulen für die jeweiligen Applikationen. Die Windowsumgebung agiert als WORKGROUP und hat nur local User.

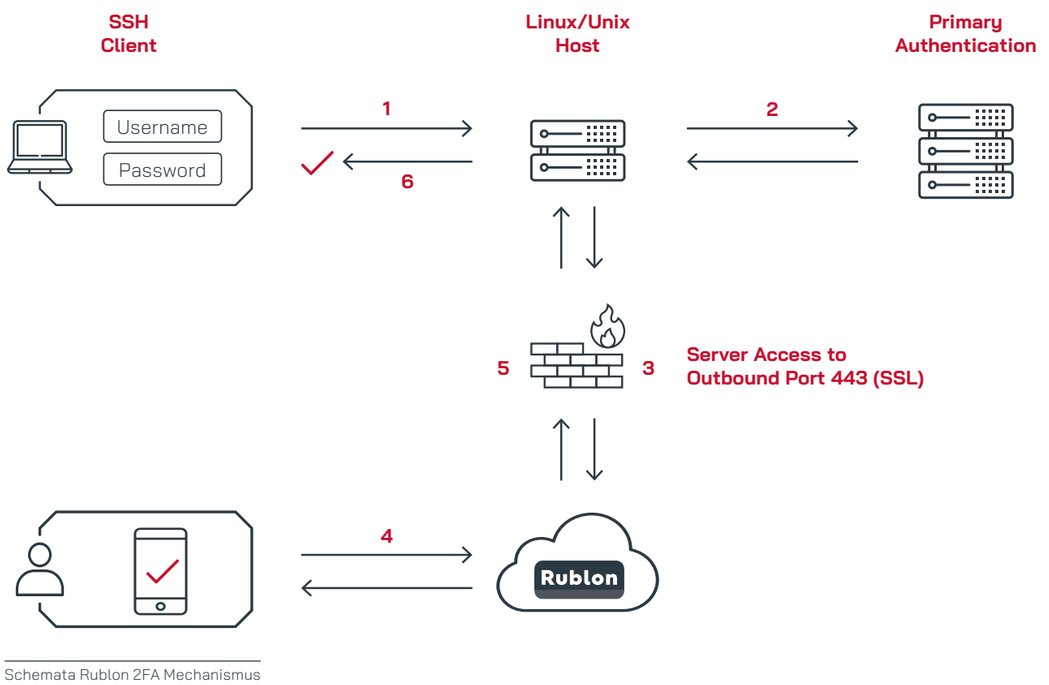
Sicherheit von administrativen Zugriffen

Durch die Verwendung einer 2-Faktor-Authentifizierung wird garantiert, dass sich keine unbefugte Person auf dem System einloggen kann. Zudem sind Logins mit dem „root“ Benutzer blockiert. ANIO verwaltet jene Benutzer, die mit dem „sudo“ Befehl administrative Aufgaben erledigen.



Welche 2FA Lösung wird verwendet?

Als 2FA Mechanismus wird die Authentifizierung für das Betriebssystem oder die Cockpit Applikation über eine Lösung der Firma Rublon implementiert. Nach dem Login gibt es eine eine *Push Notification* zu einem definierten Soft-Token, welcher vom Benutzer freigegeben werden muss. Dieser Mechanismus kann unabhängig oder auch zusätzlich zu bestehenden Mechanismen integriert werden.



Schemata Rublon 2FA Mechanismus

Wer bekommt einen Named User? Was passiert, wenn der User ‚sudo/su' macht?

Weiters wird für alle vom Kunden definierten Benutzer ein eigener Account auf den Linux und Windows Systemen angelegt. Root Zugänge sind nicht erlaubt. Root Rechte sind nur per sudo Command freigeschalten und werden nur für ebenfalls vom Kunden definierte Benutzer erlaubt. Logins und sudo Aktivitäten werden protokolliert.

Physisch statt virtuell

Die ANIO Backup Appliances laufen auf dedizierter Hardware. Dabei wird ganz bewusst auf einen virtuellen Betieb der Appliances verzichtet. Dies ermöglicht es, alle virtuellen Systeme als auch die Hosts über ein Backup vollständig zu sichern.

Die Passwörter der Remote Management Zugänge werden in einem gemeinsamen 1Password Vault hinterlegt, auf welchen der Kunde Zugang erhält.

Kann man die BIOS bzw. iDRAC Passwörter zurücksetzen?

Weiters sind die Passwörter vom Server Hersteller DELL fixiert (random – factory set), dh nach einem Reset können diese auf der dem Servern beigelegten Card eingesehen werden.

Wie lange ist die Retentiontime? Ab wann wird das Backup überschrieben?

Die Retentiontime der so gesicherten Backups kann mit der Veeam Console vom Kunden frei definiert werden.

Backup Sicherheit

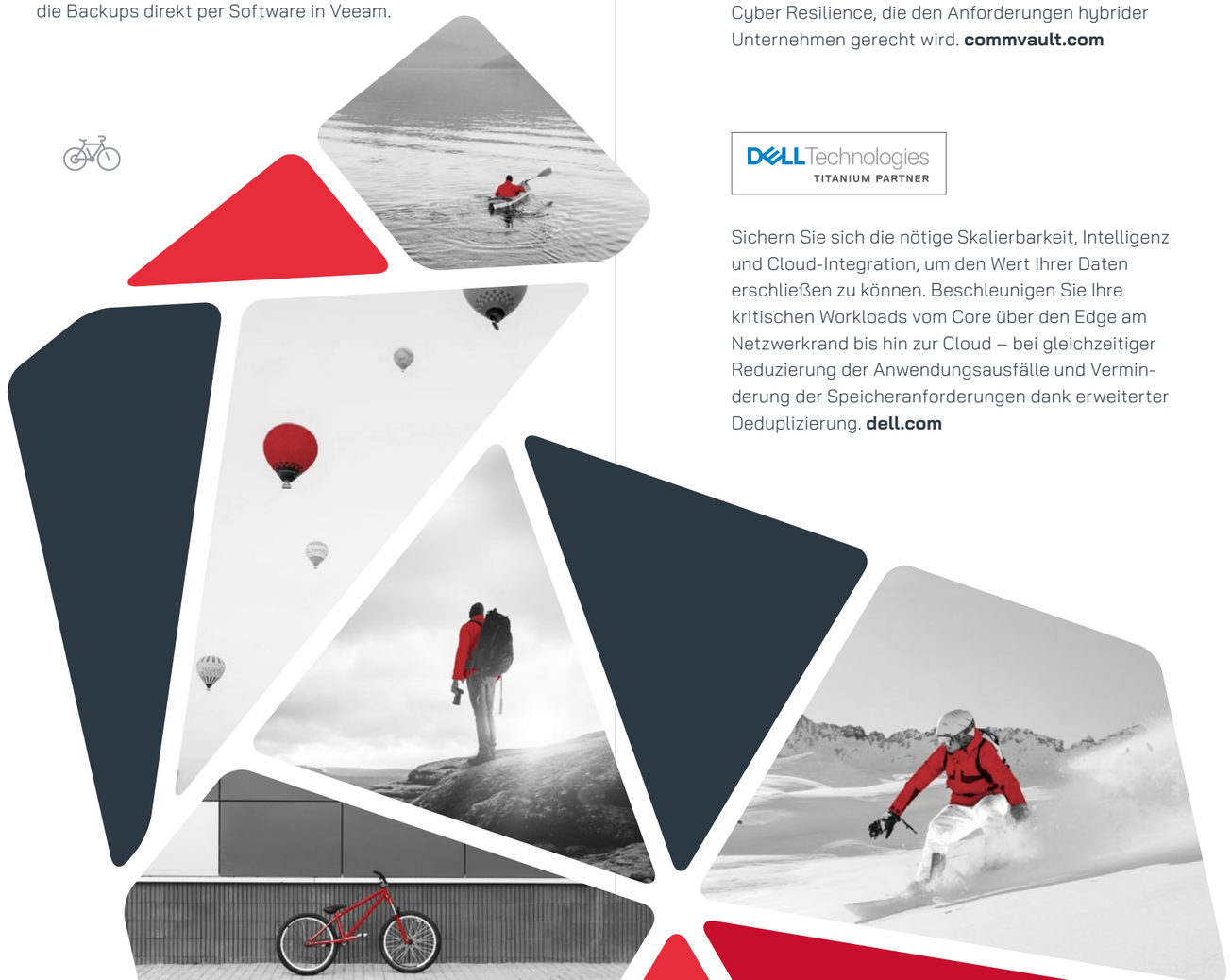
Zusätzlich zur Integrität Ihrer Backups bietet ANIO mittels Verschlüsselung die Möglichkeit, dass wirklich nur Sie Zugriff auf Ihre Daten haben. ANIO verwendet dedizierte Backup-Repositories für jeden Backup-Account. Damit ist gewährleistet, dass dieser Benutzer nur Zugriff auf die von ihm angelegten Backups hat.

WORM Technologie durch Veeam Immutability

ANIO verwendet die WORM Technologie (write once, read many) des Herstellers Veeam. Damit wird garantiert, dass die Backups für einen konfigurierten Zeitraum unveränderlich gespeichert werden, und im Falle eines Cyberangriffs unverändert bleiben.
Der Aufbau der Appliances und die Einrichtung dieses Features entspricht dem „Hardened Repository" Guide der Veeam für Repository Server.

Wie werden die Backups verschlüsselt? Algorithmus?

Die Verschlüsselung der Daten ist optional und kann auf Wunsch auf mehreren Ebenen eingeschalten werden. Für die Appliance XS und S auf OS Ebene, für die Appliance M bis XXL auf Storageebene, oder die Backups direkt per Software in Veeam.



Commvault

Zero Trust-Datensicherheit | Schnelle, unveränderliche Wiederherstellung | Die niedrigsten Gesamtbetriebskosten Commvault® Cloud, unterstützt durch Metallic® AI. Es handelt sich um eine bahnbrechende Cyber Resilience, die den Anforderungen hybrider Unternehmen gerecht wird. **commvault.com**

DELL Technologies
TITANIUM PARTNER

Sichern Sie sich die nötige Skalierbarkeit, Intelligenz und Cloud-Integration, um den Wert Ihrer Daten erschließen zu können. Beschleunigen Sie Ihre kritischen Workloads vom Core über den Edge am Netzwerkrand bis hin zur Cloud – bei gleichzeitiger Reduzierung der Anwendungsausfälle und Verminderung der Speicheranforderungen dank erweiterter Deduplizierung. **dell.com**

Red Hat
Premier
Business Partner
Solution provider
Container platform specialist

Stellen Sie IT-Services für unterschiedliche Infrastrukturen schnell und kosteneffizient bereit – mit unserem Portfolio an Lösungen für Hybrid Cloud-Infrastrukturen, Anwendungsservices, cloudnative Anwendungsentwicklung und Automatisierung. **redhat.com**

veeam
Accredited Service Partner

Bleiben Sie in Hybrid-Cloud-Umgebungen Besitzer Ihrer Daten, behalten die Kontrolle darüber und profitieren von zuverlässiger Sicherung und Wiederherstellung. Gewährleisten Sie einen stabilen Geschäftsbetrieb, schützen Sie Ihre Daten vor Angriffen und vermeiden Sie Datenverlust und Ausfallzeiten. Dank Cloud Mobility können Sie Ihre Daten ohne Festlegung auf einen Provider flexibel in die Cloud migrieren. **veeam.com**

AN.IO