WHITE PAPER | IMMUTABLE STORAGE

Mogelpackungen vermeiden und Daten unveränderbar abspeichern

RNT Rausch. Making IT possible.

RNT RAUSCH

Foto: ©Sidorov | Depositphotos.com

Mogelpackungen vermeiden

und Daten unveränderbar abspeichern

Unveränderbarer Speicher (Immutable Storage) sollte bei allen IT-Sicherheitskonzepten als letzte Verteidigungslinie gegen Ransomware-Attacken und andere Cyberangriffe stehen. Darüber hinaus sind unveränderbare Datenspeicher unverzichtbar für die Sicherung (Backup) und Archivierung von Daten. Bei Backup und Archivierung müssen darüber hinaus in sensiblen Bereichen, wie z.B. dem Finanz- oder Gesundheitswesen, strenge Datenschutzrichtlinien eingehalten werden, die deutlich über die gesetzlichen Vorschriften hinausgehen. Der Markt bietet aktuell eine Vielzahl verschiedener technischer Ansätze für Immutable Storage. Doch nicht immer sind die wertvollen Daten absolut unveränderbar gespeichert, weil oftmals Personen mit vollen Administrationsrechten trotzdem darauf zugreifen können. Ein Blick auf die technischen Details hinter der Marketing-Fassade gibt Aufschluß und schützt vor solchen Mogelpackungen. Denn im Zeitalter schnell fortschreitender technischer Evolutionen ist "Immutable Storage" nicht mehr gleich "Immutable Storage".

Die Bedrohung ist so hoch wie nie

Der aktuelle Cybersicherheit-Lagebericht "ENISA Threat Landscape 2022" (ETL 2022) der European Union Agency For Cybersecurity (ENISA) aus dem Oktober 2022 identifiziert Ransomware-Attacken sowie Denial-of-Service (DoS) Angriffe, die auf die Verfügbarkeit von Netzkomponenten ausgerichtet sind und sogar ganze Systeme zusammenbrechen lassen, als die größten Gefahren für die europäische Wirtschaft. Aufgrund der aktuellen geopolitischen Lage und der zunehmenden Professionalisierung der Hackerszene ist die Bedrohungslage so hoch wie nie. Gleichzeitig richten Cyberangriffe in einer zunehmend digitalisierten Welt immer größeren betriebs- und volkswirtschaftlichen Schaden an. Machine-Learning-Modelle bilden beispielsweise das Herzstück vieler Digitalisierungsprojekte und geraten laut ETL 2022 zunehmend ins Visier der Cyberkriminellen. Auch verteilte DoS-Angriffe auf IoT-Netze treten immer häufiger auf und blockieren beispielsweise Überwachungssysteme oder Fertigungsprozesse.

Um sich vor diesen Angriffen zu schützen, muss ein strategisches Sicherheitskonzept her - auch und vor allem für den Mittelstand. Doch ein hundertprozentiger Schutz lässt sich auch damit leider nicht gewährleisten. Über Phishing- und Supply-Chain-Attacken oder andere Social-Engineering-Methoden können sich Hacker dennoch Zugang zum IT-Netz eines Unternehmens verschaffen und dort beispielsweise Daten im Rahmen eines Ransomware-Angriffs verschlüsseln.

Ein Immutable-Storage-Sicherheitskonzept ist somit die letzte Verteidigungslinie. Denn damit sind wertvolle Unternehmensdaten beispielsweise auf WORM-Speichermedien (WORM: Write Once, Read Many) so abgespeichert, dass sie sich weder verändern, löschen oder verschlüsseln lassen. Zu den typischen WORM-Medien zählen optische Speicher wie CD-Rs, DVDs, spezielle Bandspeichertechnologien oder auch Festplattenspeicher mit einer softwarebasierten Sperre gegen das Verändern oder Löschen von Dateien. Nach einem Ransomware-Angriff kann so das IT-Team mithilfe dieser unveränderbaren Sicherung alle Daten mehr oder weniger schnell und verlustfrei von einer sauberen Backup-Kopie wiederherstellen. Lösegeldforderungen verlieren ihren Schrecken und machen die Zahlung obsolet.

Foto: ©SergeyNivens | Depositphotos.com

Die größten Cyberbedrohungen in der EU

Ransomware:
Schätzungsweise 60% der von Ransomware betroffenen Organisationen haben hohe Lösegeld-forderungen gezahlt und zum Teil trotzdem keinen vollständigen Zugriff auf alle Daten erhalten.

Malware:
2022 gab es 66 Enthüllungen von Zero-Day-Schwachstellen (Software-Schwachpunkte), die noch nicht gepatcht waren und bis zu ihrer Behebung (Zero Day) als Einfallstore für Hacker dienten.

Social Engineering:
Phishing (Versand gefälschter E-mails) ist nach wie vor eine beliebte Technik und tritt in vielfältigen Formen auf: gezieltes Spear Phishing per E-Mail, Whaling bei Führungskräften, Smishing per Messenger oder Vishing via Anruf.

Angriffe auf Daten:
Diese steigen proportional zur Gesamtmenge der produzierten Daten an.

Angriffe, die die Verfügbarkeit der IT bedrohen:
Von DoS- und DDoS-Attacken geht die größte Bedrohung aus. Die Verfügbarkeit des Internets wird durch die Zerstörung der Infrastruktur oder Störungen und Umleitungen des Internet-Traffics bedroht.

Desinformation/Fehlinformation:
Vor allem Medien und Social-Media-Plattformen sind Ziel von KI-gestützter Desinformation, Deepfakes (täuschend echt wirkende, manipulierte Bild-, Audio- oder Videoaufnahmen) und Desinformation-as-a-Service.

Supply-Chain-Angriffe:
Diese Angriffsvariante nimmt stark zu. Angreifer dringen über Drittanbieter oder Lieferanten in die Lieferkette oder das Netzwerk eines Unternehmens ein. Im Berichtszeitraum gingen 17% der Einbrüche auf Supply-Chain-Angriffe zurück, im Vorjahr waren es noch weniger als 1%.

Quelle: ENISA Thread Landscape 2022

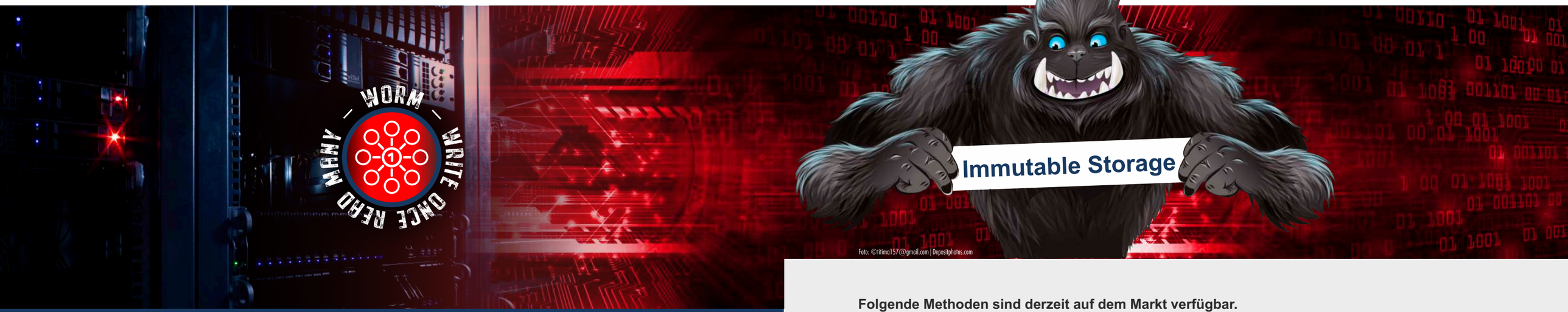

Foto: ©titima157@gmail.com | Depositphotos.com

Immutable Storage
zum Schutz wertvoller Daten

Technisch gesehen schiebt Immutable Storage der Verschlüsselung, Löschung und Veränderung von Daten einen Riegel vor. Das umfasst nicht nur Angriffe von außen, sondern auch versehentliche oder absichtliche Manipulationen durch Mitarbeitende innerhalb eines Netzwerkes.

Bis vor einigen Jahren erfolgte die Datenspeicherung unveränderbar nach dem WORM-Prinzip auf speziellen Medien. Dieses Prinzip wird aber für viele IT Umgebungen im Zeitalter der digitalen Transformation schnell zu teuer. Zudem werden diese Medien auch meist mit dem enormen Datenwachstum aus zeitlichen und/oder Kapazitätsgründen den aktuellen Anforderungen an eine flexible und skalierbare Infrastruktur nicht mehr gerecht. Der Kostenfaktor spielt hier natürlich auch eine wesentliche Rolle.

Für eine moderne digitale Welt sind anwendungsbezogene monolithische Datensilos in starren hierarchischen Strukturen somit nicht mehr geeignet. Deshalb werden Daten zunehmend objektbasiert als unstrukturierte Datenpools auf Software-Defined-Storage (SDS) Systemen - vor Ort und in der Cloud - abgespeichert. Im Gegensatz zu herkömmlichen Speicherarchitekturen, bestehend aus proprietären Kombinationen von Herstellern spezifischer Hard- und Software, entkoppelt SDS diese Abhängigkeiten. Die Hardware wird von einem abstrahierten Software Layer angesprochen, der unter anderem festlegt, wie und wo die Daten zu speichern sind. Somit wird der Einsatz kostengünstigerer Standard-Hardware von einem Hersteller der Wahl möglich.

Diese so wichtigen technischen Weiterentwicklungen erfordern eine Erweiterung der ehemals recht eindeutigen Definition von Immutable Storage, denn die Unveränderbarkeit von Daten findet bei SDS nicht mehr nur auf dem Hardware Layer statt.

Folgende Methoden sind derzeit auf dem Markt verfügbar.

① Hardware WORM: klassisch

Bei Hardware-WORM arbeitet die Speicherhardware ausschließlich nach dem WORM-Prinzip. Dabei handelt es sich meist um optische, nur einmal beschreibbare Medien wie CD-Rs oder Ultra Density Optical (UDO) Medien, die im digitalen Zeitalter als Datenträger aus der Mode gekommen sind. Allerdings haben unlöschbare Tapes immer noch ihre Anwendungsbereiche. Alle hier beschriebenen Medien verfügen über nur wenig Speicherkapazität, die nach dem ersten Beschreiben mit Daten dauerhaft blockiert ist. Die Datensätze können nach der Aufbewahrungsfrist nicht mehr gelöscht werden, es bleibt nur die physikalische Zerstörung.

② Systemischer WORM: klassisch

Beim systemischen WORM sind Controller, Prozessoren oder Adressierungsverfahren darauf ausgelegt, dass sie die Daten unveränderbar und nicht löschbar auf einem Medium abspeichern und damit einmalige Beschreibbarkeit ermöglichen. So kann zum Beispiel der integrierte Prozessor eines USB-Sticks die WORM-Eigenschaft herstellen.

③ Systemischer WORM: Content-Addressed Storage

Für große Datenmengen bietet sich der systemische WORM-Speicher CAS (Content-Addressed Storage) an. Ein dediziertes Festplattensystem speichert die Informationen in eindeutig zugeordneten Objekten ab, die wiederum in einem festgelegten Bereich einer Festplatte zusammen mit diesem Speicherort abgelegt werden. Würde sich der Inhalt der Datei nachträglich verändern, hätte dies einen anderen Speicherort zur Folge. Die Löschung der Objekte gelingt erst nach Ablauf einer bestimmten Aufbewahrungsfrist.

④ Systemischer WORM: Continuous Snapshots

In ähnlicher Weise können auch Continuous Snapshots (kontinuierliche Datensicherung) vor Ransomware-Angriffen schützen. Das Speicher-system erstellt die Kopien (Snapshots) automatisch in festgelegten Abständen und speichert sie als eigenständige Objekte ab. Zur Zeit kann Ransomware nur aktive Objekte verschlüsseln. Das macht den vorherigen Snapshot unangreifbar, was den maximalen Datenverlust auf wenige Sekunden reduziert. Allerdings legt das Speichersystem bei Änderungen oder Löschungen neue Snapshots an, die weiteren Speicherplatz brauchen.

Dieses Verfahren eignet sich zum Beispiel für Echtzeitanwendungen, wie zum Beispiel in den Bereichen Internet of Things (IoT) oder Industry 4.0, ist aber für langfristig gespeicherte Daten, die kaum verändert werden, ein teurer Weg.

⑤ Software – WORM für die Archivierung

Bei Software-WORM-Storage erzeugt eine spezielle Soft- oder Firmware die "Write Once, Read-Many"-Eigenschaft für das Speichermedium, indem es die Attribute simuliert, die physikalische Speichermedien wie Festplatten oder LTO-Bänder unveränderbar machen. Einen direkten Zugriff auf das Speichermedium unter Umgehung der Software verhindert beispielsweise eine Datenverschlüsselung. Manipulationssicherheit erreichen Software-WORMs unter anderem per Datensicherung über elektronische Quittungen (Hash-Codes). Dabei wird die Systemzeit mit einem verifizierten Zeitserver (Time-Sync) synchronisiert. So wird erreicht, dass:

- Zugriffs- und Leserechte dokumentiert sind
- Daten nur einmalig geschrieben werden können
- Niemand Daten löschen kann
- Jeder mit entsprechenden Berechtigungen Daten bei Bedarf lesen kann

Dateien lassen sich so dauerhaft oder bis zum Ablauf der Aufbewahrungsfrist vor Veränderung schützen. Viele Archivierungslösungen nutzen diesen Ansatz bereits und lösen so das Problem der Skalierbarkeit in punkto Hardware bei weiterhin explodierenden Datenmengen. Doch aufgepasst - mit Administratorenrechten gelingt trotzdem eine Verschlüsselung, Löschung oder Veränderung der Daten.

⑥ WORM – konformer Objektspeicher - S3 Object Lock

Alle Object Storage Lösungen mit nativer S3 Schnittstelle haben Zugriff auf die integrierte Object Lock Funktionalität, die bereits jetzt schon inoffizieller Industriestandard für unveränderlichen Objektspeicher ist. Das gilt nicht nur für die Cloud sondern auch für lokale Lösungen. Object Lock eignet sich perfekt für

- Den Schutz vor Ransomware
- Archivierung mit gesetzlichen Aufbewahrungsfristen
- Speicherung, Backup oder Archivierung besonders sensibler Daten unter weiteren regulatorischen Anforderungen

Viele Anbieter von Backup Softwarelösungen unterstützen die Object Lock Funktion bereits nativ. Beim Objektspeicher werden Daten als Objekte gespeichert, die wiederum in sogenannten Buckets organisiert werden und alle Metadaten enthalten. Object Lock hat unterschiedliche Einstellungen zum Schutz der Daten und macht es innerhalb eines vorab definierten Zeitraums unmöglich Objekte oder Buckets zu löschen, zu überschreiben oder zu verschlüsseln. Im Compliance Mode können selbst Anwender mit Root-Admin- Zugangsrechten an mit Object Lock geschützen Daten nicht herumpfuschen.

Gerichtsfeste Aufzeichnung von Daten mit S3-Object-Lock

Desweiteren ermöglicht Object Lock zum Beispiel die gerichtsfeste Aufzeichnung von Videoaufnahmen oder Gesprächen. So haben Polizei oder auch Feuerwehren bereits kompakte Object Storage Appliances mit integrierter Object Lock Funktionalität im Einsatz, um Videoaufzeichnungen von Bodycams oder Drohnen gerichtsfest abzuspeichern. Die Object Lock Funktion verhindert eine nachträgliche Manipulation dieser Videos. Bei dem S3-SDS-Cloudian-Hyperstore-Objektspeicher ist die Object Lock Funktion sogar so restriktiv voreingestellt, dass selbst Menschen mit Root-Admin-Zugangsrechten die abgespeicherten Originaldaten im festgelegten Zeitraum weder verändern, noch löschen oder anderweitig manipulieren können. In ähnlicher Weise ist es möglich, Gespräche in Notariaten, bei Gericht oder in Rechtanwaltskanzleien ebenso gerichtsfest aufzuzeichnen, wie ärztliche Untersuchungsergebnisse beim Verdacht auf Misshandlung, Vergewaltigung oder Körperverletzung.

RNT RAUSCH

Foto: © vska | Depositphotos.com

Die Qual der Wahl

Alle hier vorgestellten Immutable-Storage-Lösungen weisen Stärken und Schwächen auf.

Im Fall von weitgehend virtualisierter Unternehmens-IT kommt Hardware-WORM nicht mehr infrage. Archivierungslösungen mit Software-WORM oder auch einige systemische WORM-Speichervarianten ermöglichen über einen Administrationszugang dennoch eine Verschlüsselung der Daten. Manche Verfahren eignen sich vor allem aus finanzieller Sicht eher für agile Anwendungen, andere für die revisionssichere Archivierung. Wer eine Lösung sucht, die Daten tatsächlich unveränderbar und revisionssicher abspeichert, kann nur auf klassische WORM-Medien zurückgreifen - oder auf SDS-Systeme, die auf S3 mit Object Lock basieren.

WORM–Methode	SICHERHEITSNIVEAU	EIGENSCHAFTEN
Hardware–WORM	★★★★★★	offline, niedrige Kapazität, aufwendig
Systemischer WORM klassisch	★★★★★★	offline, niedrige Kapazität, aufwendig
Content-Addressed Storage	★★★☆☆☆	online, objektbasiert, Herstellerlösung, für bestimmte Festplatten, Admin-Zugriff absichern
Continuous Snapshots	★★★☆☆☆	online, objektbasiert, Herstellerlösung, Admin-Zugriff absichern, für agile Anwendungen als Ransomware-Schutz
Software–WORM	☆☆★★★☆	online, je nach Zugriffsmöglichkeiten des Admin + Schutz vor Datenklau, vor allem für Archivierung
Amazon S3–Object–Lock	★★★★★☆	online, für revisionssichere, rechtsfeste Datenspeicherung und Archivierung plus Ransomware-Schutz, offener Standard

Immutable Storage
zur Erfüllung rechtlicher Auflagen

Ein weiterer Vorteil von Immutable Storage ist neben der Erfüllung rechtlicher Auflagen auch die Revisionssicherheit, sodass Unternehmen wichtige Dokumente, wie zum Beispiel Verträge oder Bankunterlagen, revisionssicher aufbewahren und unveränderbar digital speichern können. Buchhaltungsdaten erfordern beispielweise eine zehnjährige Aufbewahrung. § 239 des Handelsgesetzbuchs (HGB) schreibt hierzu Folgendes vor: "Die gespeicherten Dokumente müssen unveränderbar, reproduzierbar und jederzeit verfügbar sein." Auch bei steuerlich relevanten Daten gilt ausnahmslos, dass sie in allen Varianten unveränderlich abgespeichert werden müssen. Die Datenschutzgrundverordnung (DSGVO) schreibt darüber hinaus die filigrane Definition der Zugriffsrechte auf Personendaten vor, um diese vor unbefugtem Zugriff, Datenmissbrauch oder -verlust zu schützen. Für all diese Zwecke bietet der Markt verschiedene Archivierungslösungen an, die auf Immutable Storage Lösungen basieren und über den betreffenden Software Layer einen sicheren und rechtskonformen Betrieb sowie Datenhoheit gewährleisten.

Fazit:
Hundertprozentige Sicherheit gibt es nicht

Alle Varianten, außer Hardware-WORM, basieren letztlich auf Software und sind deshalb nie zu 100 Prozent sicher. Das gilt selbst für S3 Object Lock. Sicherheitslücken in Software und Hardware können unter Umständen jeden Überschreibschutz umgehen. Doch wer agiles SDS betreibt, kann die anfallenden Datenberge schlicht und ergreifend nicht auf CD-Rs speichern. Wer eine Immutable Storage Lösung einsetzen will, muss sich darüber im Klaren sein, dass jede Möglichkeit das Read-only-Attribut zu verändern die Gefahr beinhaltet, dass ein Hacker sich Administrationsrechte verschafft und das System manipuliert. Deshalb gehören zu jedem Cyber Security Konzept grundsätzlich stringente Massnahmen, wie z.B. ein Zero-Trust-Ansatz und Multi-Faktor-Authentifizierungen, die für alle Administratoren und Anwender im Unternehmen gleichermaßen gelten.

Im Zeitalter der digitalen Transformation und der damit einhergehenden schnellen technischen Evolution sind moderne und zukunftssichere Lösungen darauf ausgelegt, weit mehr als höchstmöglichen Schutz der Daten zu bieten. Vor allem bei hybriden Ansätzen sind IT-Entscheider gut beraten darauf zu achten, dass die für ihr Unternehmen optimale Lösung auch im Hinblick auf die Nutzung der Cloud alle die relevanten Verordnungen einhält. Dazu gehören neben der DSGVO auch die Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern sowie Aufzeichnungen und Unterlagen in elektronischer Form (GoBD). Im internationalen Umfeld sind zum Beispiel die Vorgaben der US-amerikanischen Aufsichtsbehörde SEC oder der Schweizer FinSA relevant. Hinzu kommen noch branchenspezifische Richtlinien, etwa für die Bereiche Gesundheit, Chemie, Finanzen oder Automobilbau.

Weitere Informationen zu den Immutable-Storage-Appliances von RNT Rausch finden Sie hier.

Mit diesem Click sehen Sie unsere Cloud Bundles, die eine Yowie Appliance mit Cloud Storage Made in Germany im Abomodell kombiniert.

RNT RAUSCH

RNT Rausch GmbH
WHITE PAPER
IMMUTABLE STORAGE

RNT Rausch. Making IT possible.

RNT Rausch ist ein in Deutschland ansässiger Technologiepionier mit mehr als 20 Jahren Erfahrung in der Hightech-Server- und Storage Branche. Das Unternehmen entwirft zukunftssichere Server- und Storagelösungen, die hybride Architekturen ermöglichen und geschäftliche Herausforderungen meistern, um KMUs, Unternehmen, Rechenzentren und Service Provider auf der ganzen Welt fit für die technische Revolution von morgen zu machen. RNT bietet personalisierte Lösungen und maßgeschneiderte Dienstleistungen, die den Kunden helfen, Sicherheit, Flexibilität, Skalierbarkeit und Nachhaltigkeit zu verbessern.

Mehr als 30 Mitarbeiter liefern zielgerichtete Lösungen, die mit äußerster Präzision und in höchster Qualität vor Ort gefertigt werden.

Weitere Informationen

finden Sie unter https://rnt.de

RNT Rausch. Making IT possible.

RNT Rausch GmbH
Im Stöck 4a | 76275 Ettlingen | Germany

Phone: +49 7243 5929-0 | Fax +49 7243 5929-14
Mail: info@rnt.de | https://rnt.de