Cloud Storage Security

Massendaten in der Cloud schützen: Wie S3 Object Storage zu einer sicheren Bank wird

Herausforderungen und Maßnahmen für Object Storage als bestens geschützter Massenspeicher

White Paper

IONOS

Executive Summary

- Im Storage sind geeignete technische Maßnahmen umzusetzen, um Industriespionage, Sabotage und Datendiebstahl zu unterbinden.
- S3 Compatible Storage ist eine bewährte Alternative zum Objektspeicherdienst AWS S3 von Amazon, dass als US-Unternehmen dem US CLOUD Act unterliegt.
- S3 Compatible-Storage-Lösungen sind standardisierbar und zeichnen sich durch sehr gute Skalierbarkeit, maximale Ausfallsicherheit und eine einfache Handhabung aus.
- Ein sehr detailliertes und restriktives Rechtemanagement sorgt für den hohen Datenschutz im S3 Compatible Storage.
- Dank Versionierung lassen sich Datenverluste durch Bedienfehler weitestgehend vermeiden.

Inhalt

1 Einführung

In Zeiten von DSGVO und US CLOUD Act wird zurecht regelmäßig die Bedeutung der gesetzgeberischen Vorgaben zur Datensicherheit im Cloud Computing betont. Beispielsweise finden sich im Whitepaper „Streitfrage CLOUD Act – Auswirkungen auf Datenschutz und Datensicherheit in Deutschland und Europa“ Informationen zur aktuellen Rechtslage. Whitepaper

Sicherheit hat neben dem rechtlichen Aspekt jedoch auch eine technische Seite. Insbesondere hinsichtlich Object Storage werden immer wieder technische Sicherheitslücken offenkundig, die die Datensicherheit der Unternehmen ernsthaft bedrohen. Kriminelle nutzen vorhandene Schwachstellen, um Daten zu entwenden oder zu sabotieren; betroffene Unternehmen riskieren zudem eine beschädigte Reputation. S3 Object Storage weist jedoch sehr große Vorteile gegenüber anderen Speicherarten auf. Dazu gehören deutlich geringere Speicherkosten und eine hohe Flexibilität. Die Lösung besteht daher nicht darin, auf diese Technologie zu verzichten, sondern die technische Sicherheit von S3 Object Storage Daten signifikant zu erhöhen. Das vorliegende Whitepaper zeigt, wo die Knackpunkte in puncto Sicherheit sind und stellt geeignete Maßnahmen vor, die sich in der Praxis bereits bewährt haben.

2 Cyberkriminalität und Nachlässigkeit gefährden deutsche Unternehmen

2.1 Der unmittelbare wirtschaftliche Schaden

Der wirtschaftliche Schaden, der durch Industriespionage, Sabotage und Datendiebstahl entsteht, ist immens. Zumal die Cyberangriffe in jüngster Zeit stark zugenommen und bei 70 Prozent der betroffenen Unternehmen auch einen Schaden verursacht haben. Darauf verweisen Bitkom sowie Verfassungsschutz und beziffern die jährliche Schadenssumme allein für Deutschland auf über einhundert Milliarden Euro. Dabei sind Folgeschäden, etwa Image- und Vertrauensverluste und ein damit verbundenes Abwandern von Kunden, noch nicht eingerechnet.

Die höchsten Schäden haben demnach Angriffe auf Passwörter, das Infizieren mit Schadsoftware und Phishing-Angriffe zu verantworten – Risiken, die nicht nur für Webseiten, sondern auch im Storage-Bereich vorhanden sind.

Cloud überholt Unternehmensserver

Unternehmen haben immer mehr zu verlieren, denn schließlich befinden sich mittlerweile ganz erhebliche Datenmengen in der Cloud – Tendenz weiter steigend: Dem Internetportal Statista zufolge wird die Cloud dieses Jahr (2020) die On-Premises-Speichermedien überholen. Auch IT-Workloads sind im großen Stil migriert, Stichworte sind SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service), IaaS (Infrastructure-as-a-Service) und Storage.

2.2 Im Fokus der Angreifer: die Public Cloud der Global Player

Die Zahlen der Cloud Threat Reports 2019 und 2020 von Palo Alto Networks, Inc. sprechen für sich:

- Kundenanwendungen allein auf AWS, Azure und GCP weisen über 34 Millionen Sicherheitslücken auf – etwa in Form veralteter Apache-Server und anfälliger jQuery-Pakete.
- Mehr als 43.000 Container-Plattformen, überwiegend Docker- und Kubernetes-Container, haben Standardkonfigurationen, die sich mit einfachsten Suchbegriffen identifizieren lassen und so einen nicht authentifizierten Zugriff auf die Daten gewähren.
- Fast ein Drittel der Unternehmen kommuniziert mit Malware (Cryptomining-C2-Domains).
- Es sind über 199.000 unsichere Templates im Einsatz.
- Nahezu 45 Prozent der Cloud-Datenbanken sind unverschlüsselt.
- 60 Prozent der Cloud-Dienstleister protokollieren nicht. Wie groß ein möglicher Schaden durch einen Sicherheitsvorfall ist, lässt sich damit nicht nachvollziehen.

Ursache für mehr als die Hälfte der gemeldeten Sicherheitsvorfälle waren Fehlkonfigurationen, ein Viertel geht auf kompromittierte Accounts zurück

2.3 „Nur“ aus Versehen? Das macht es nicht weniger schädlich.

Nicht nur kriminelle Akte bedrohen die Geschäftsfähigkeit und Solvenz von Unternehmen. Auch die Sorglosigkeit von Mitarbeitern im Umgang mit sensiblen Daten sowie technische Pannen können sehr ernste Konsequenzen nach sich ziehen: Der Ruf als zuverlässiger Partner nimmt nachhaltig Schaden, und in der Regel bedarf es großer Anstrengungen und viel Zeit, um verloren gegangenes Vertrauen der Kunden neu aufzubauen. Vom Begleichen möglicher Ersatzforderungen der Geschädigten oder Strafzahlungen wegen der Verletzung datenschutzrechtlicher Vorgaben ganz zu schweigen.

Augen auf bei der Rechtevergabe

Ein typisches Defizit ist die zu großzügige Vergabe von Zugriffsrechten, die zu einer unbeabsichtigten Preisgabe von Daten führen, die eben nicht zur Offenlegung oder Weitergabe bestimmt sind. Auch für Fehler bei der Softwarekonfiguration gibt es genügend Negativbeispiele. So konnte man etwa vor einigen Jahren im Internet auf zehntausende hochsensible Kundendaten der National Credit Federation zugreifen. Der Grund: ein frei verfügbarer sogenannter Bucket im Object Storage – einer immer populärer werdenden Form der Speicherung von Massendaten.

3 Object Storage: Innovative Speicherlösung oder Einfallstor für Kriminelle?

3.1 State of the Art

Das Datenaufkommen in den Unternehmen steigt unaufhörlich: von Dokumenten über E-Mails und Nachrichten bis hin zu Bild- und Videodateien. Doch viel zu oft noch legt man sie unstrukturiert und dezentral ab. Die Folge sind nicht nur hohe Speicherkosten, es gibt auch ein erhöhtes Risiko für Datenverlust und -diebstahl.

Eine elegantere Speicherlösung ist daher Object Storage. Der große Vorteil im Vergleich zu anderen Storage-Möglichkeiten: Da die Datei zusammen mit den zugehörigen Meta-Daten gespeichert wird, lässt sich ihr Inhalt näher beschreiben, was das Strukturieren und Verwalten großer Mengen unstrukturierter Daten erheblich vereinfacht. Ordnerstrukturen mit ihrem hierarchischen Prinzip fallen weg. Weitere Pluspunkte von Object Storage sind seine quasi uneingeschränkte Skalierbarkeit und hohe Flexibilität sowie die Möglichkeit, ihn online übers Web per https, über ein Nutzerportal bzw. einen entsprechenden Client systemübergreifend in jeden Workflow einzubinden.

Stateless Container und Cloud

Nahezu unendlich skalierbar und unabhängig vom Client-Dateisystem – insbesondere diese beiden Eigenschaften machen Object Storage zur bevorzugten Speicherlösung für Stateless Container und für die Cloud. Große Datenmengen lassen sich flexibel und kostengünstig speichern und gegenseitig austauschen, wo sich die Daten physisch befinden, ist für den Anwender unerheblich. Unternehmen nutzen Object Storage daher vor allem als Backup-Target, für die Notfallwiederherstellung und zur dauerhaften Archivierung von Daten. Als Medienarchiv oder zum Erfassen von Sensordaten im IoT gewinnt die Speicherlösung zudem immer mehr an Bedeutung in Hinblick auf Big Data und Machine Learning.

3.2 Der S3-Standard und seine Doubles

AWS S3-kompatibler Object Storage hat sich de facto als inoffizieller Standard für Cloud Storage Services im Massendatenbereich etabliert und dominiert das öffentliche Cloud Computing für beispielsweise Online Backups und zum Archivieren von Daten und Applikationen. Er punktet unter anderem mit seiner sehr robusten Verwaltungsschnittstelle für Daten, die es im Gegensatz zu herkömmlichen Dateisystem-Schnittstellen erlaubt, Daten über einen umfangreichen API-Satz (API – application programming interface) zu steuern und in automatisierte Prozesse zu integrieren. Eine redundante Datenspeicherung auf mehreren Storage-Knoten sorgt für maximale Ausfallsicherheit: Durch die Replikation lassen sich Daten ohne zusätzlichen Aufwand im Bedarfsfall jederzeit wiederherstellen.

Allerdings gibt es auch Bedenken, dem Objektspeicherdienst S3 des US-Riesen Amazon oder auch weiteren Unternehmen mit Sitz in den USA sensible Daten wie Geschäftsgeheimnisse, technisches Know-how oder personenbezogene Daten anzuvertrauen. Zudem stehen dem oft rechtliche Anforderungen der EU an Datenschutz oder -sicherheit entgegen, Stichwort: DSGVO. Das Dilemma lässt sich jedoch lösen: mit S3 Compatible Storage.

Freie, kompatible Alternativen: S3 Compatible Storage

S3 Compatible-Storage-Lösungen basieren auf der Amazon S3-Programmierschnittstelle, sind damit standardisierbar und besitzen die gleichen Vorteile wie AWS S3: eine ausgezeichnete Skalierbarkeit, um die Arbeitslast beim Erweitern der Speicherkapazität nicht ändern zu müssen, maximale Ausfallsicherheit und eine einfache Handhabung. Es lassen sich beliebig große, statische Datenmengen kostengünstig speichern und via REST (Representational State Transfer) API komfortabel in automatisierte Prozesse einbinden bzw. über den Webbrowser abrufen. Der Zugriff auf die Daten und ihre Verwaltung erfolgen über S3-kompatible Schnittstellen.

Zahlreiche Backup-Programme nutzen S3, denn die Lösung ist mit ihrer hohen Interoperabilität und Kompatibilität besonders nutzerfreundlich. Die Unternehmen können flexibel auf individuell wechselnde Bedarfe reagieren und zahlen nur die Speicherkapazität, die sie real wirklich genutzt haben. So lassen sich die Speicherkosten gegenüber Cloud Block Storage um rund 60 Prozent reduzieren. Speicherplatz ist nahezu grenzenlos vorhanden und lässt sich mit verteilten Zugriffsrechten und systemübergreifend einbinden.

Es gibt verschiedene Anbieter für Cloud-Speicherdienste mit S3 API. Bei der Auswahl sollte man darauf achten, dass die Lösung clusterfähig ist. Nur so lässt sich ein System aufbauen, das die Speicherobjekte auf mehrere virtuelle Server aufteilt und damit die Ausfallsicherheit erhöht sowie eine redundante Sicherung erst möglich macht. Zudem müssen sie den Compliance-Regeln der Unternehmen, dem Datenschutz nach DSGVO und deutschen Datensicherheitsstandards gerecht werden.

3.3 Wie sicher ist S3-kompatibler Object Storage?

Viele der in Kapitel 2.2 vorgestellten Risiken der Public Cloud treten im S3-kompatiblen Object Storage per se nicht mehr auf, etwa veraltete Apache-Server, standardkonfigurierte Docker- und Kubernetes-Container und unverschlüsselte Datenbanken. Anders steht es um menschliches Fehlverhalten wie zu große Laxheit im Umgang mit Daten und die Missachtung von Sicherheitsregeln. Dem kann man allerdings mit verschiedenen technischen Mitteln wirkungsvoll begegnen.

Das eigentliche Sicherheitsproblem ist der Mensch.

4 Wirksame Maßnahmen zum Schutz vom S3-kompatiblen Object Storage

4.1 Kein Zugriff für Unbefugte

Der S3-Standard enthält bereits so genannte Permissions für Buckets und Objekte. Dabei wird zwischen dem Lese- und Schreibzugriff unterschieden: Readable bedeutet, dass sich der Nutzer die Inhalte von Buckets auflisten und Objekte anzeigen bzw. herunterladen kann. Die Berechtigung „Writable“ erlaubt es, Objekte im Bucket zu erstellen, zu verändern und zu löschen. Und schließlich gibt es noch ACP Readable und ACP Writable, um die Lese- und Schreibrechte für Buckets und Objects zu ändern. Ordner hingegen haben keine Zugriffsberechtigungen. Bei den Berechtigten unterscheidet man zwischen:

- **Public:** Jeder, ohne Einschränkungen
- **Authenticated Users:** Jeder mit einem beliebigen Account in dem Object Storage
- **Account:** Explizit angegebener User mit einem Object Storage Account
- **Owner:** Besitzer, derjenige, der das Buckets bzw. Objekt erstellt hat. Dieser hat immer den vollen Zugriff auf alle eigenen Buckets und Objekte.

Standardmäßig sind die Berechtigungen für neue Buckets und Objekte so eingestellt, dass zunächst nur der Besitzer Zugriff auf diese hat. Damit ist es nicht möglich, dass es aus purer Vergesslichkeit zu einem Sicherheitsleck kommt. Man sollte nachträglich nur im wirklichen Bedarfsfall und auch nur im unbedingt erforderlichen Umfang entsprechende Berechtigungen erteilen. Buckets, die im Object Storage zu hinterlegen sind, bieten zusätzlichen Schutz: Mit ihnen lassen sich Berechtigungen detaillierter vergeben als durch die Permission der ACL und notfalls sogar erzwingen.

Die Vergabe von Zugriffsrechten ist restriktiv zu handhaben.

Eine Funktion, um Rechte zu vererben, ist standardmäßig in S3 nicht vorhanden. Sollte ein separater S3-Client diese Funktionalität als individuelles Feature bereitstellen, ist zwingend darauf zu achten, dass nicht bestehende Rechte rekursiv überschrieben werden und so Objekte in die falschen Hände gelangen können.

Objektzugriff für nicht registrierte Anwender

Es ist gar nicht so selten, dass nicht registrierten Nutzern bestimmte Objekte zugänglich zu machen sind. Selbstverständlich darf es sich dabei nicht um vertrauliche oder sensible Daten handeln. Der Zugriff erfolgt über den Public URL Access. Er ist für jedes entsprechende Objekt in den Properties zu aktivieren. Aus Sicherheitsgründen sollte man den Zugriff durch eine Verfallszeit oder hinsichtlich der Anzahl an Downloads begrenzen.

4.2 Verlusten vorbeugen

Der Verlust von Daten ist der GAU für Unternehmen. Wenn über Nacht die patentreifen Forschungsergebnisse oder sämtliche Kundeninformationen nicht mehr verfügbar sind, kann das das Aus bedeuten. Nicht besser sieht es aus, wenn mit den Daten ein wesentlicher Bestandteil der Geschäftstätigkeit verloren geht. So 2019 geschehen, als dem sozialen Netzwerk Myspace während eines vollkommen missglückten Serverumzugs sämtliche Fotos, Videos und Musikdateien abhandengekommen sind, die Nutzer von 2003 bis 2016 hochgeladen hatten, und die sich mangels Backups nicht wiederherstellen ließen.

Ein Datenverlust kann vielerlei Ursachen haben. Zum einen sind sie eher technischer Natur, wie:

- Hardwareausfall
- ‚Data rotting', also ein schleichender Verfall der elektrisch oder magnetisch gespeicherten Bits
- Brand und andere Ereignisse, die die Hardware des Object Storage beschädigen
- Softwarefehler

Diesen Fehlerquellen kann man bis zu einem gewissen Grad entgegenwirken, indem man zum Beispiel das Redundanz-Level erhöht, Daten regelmäßig neu schreibt oder Software intensiv testet.

S3-kompatiblen Object Storages bügeln menschliche Schwächen aus.

Schwerwiegender sind menschliche Fehler oder bewusste Manipulationen. So können sowohl den Administratoren als auch den Anwendern Bedienfehler unterlaufen. Dabei spielen Unwissenheit, Unachtsamkeit und auch die Unbedarftheit der Nutzer eine unrühmliche Rolle. Dazu kommt Sabotage von außen, etwa durch Konkurrenten oder ‚digitale Vandalen', und von innen, z. B. durch frustrierte Mitarbeiter. Fehlende Kontrollmechanismen bzw. -maßnahmen begünstigen Fehlverhalten.

Datenverlusten durch Bedienfehler kann man mittels Objekt Storage in gewissen Grenzen vorbeugen. Zwar ist das Löschen oder Überschreiben eines Objektes per se irreversibel – das vorher vorhandene Objekt wird ohne weitere Prüfung gelöscht bzw. ersetzt und kann nicht wiederhergestellt werden. Selbst geo-redundante Systeme helfen hier nicht, da auch der Löschvorgang repliziert wird. Durch die in S3-kompatiblen Object Storages implementierte Versionierung besteht allerdings zumindest eine teilweise Absicherung, da die vorige Version bzw. Versionen erhalten bleiben. Dies beansprucht allerdings mehr Speicherplatz, der sich finanziell bemerkbar macht. Das führt wiederum dazu, dass die Anzahl der alten Versionen begrenzt wird, nicht selten auf eine einzige vorherige Version. Doch Vorsicht: Wird der falsche Vorgang wiederholt – sei es durch einen ungeduldigen User, durch Willkür oder auch eine fehlerhafte Software – gibt es auch keinen alten Stand, auf den man zurückgreifen kann.

Ein weiterer, für den unerfahrenen Benutzer nicht leicht erkennbarer Stolperstein ist die Benutzerverwaltung. Einerseits soll die Rechtevergabe möglichst restriktiv erfolgen. Andererseits muss jedoch sichergestellt werden, dass der vollständige Zugriff auf die Daten jederzeit möglich ist, auch wenn z. B. der zuständige Administrator das Unternehmen verlässt und sein Benutzerkonto gelöscht wird. Anders als bei einer Festplatte, die im Notfall über ein anderes System ausgelesen werden kann, sind beim S3-kompatiblen Object Storage die Zugangsdaten unerlässlich, um auf die Daten zugreifen zu können. Sollte es also Daten geben, die nur einer Person zugänglich sind, müssen die entsprechenden Zugangsdaten immer noch verfügbar und nutzbar sein.

Trotz aller Gegenmaßnahmen muss man sich immer wieder eines vor Augen führen: Ganz ausschließen lassen sich die Ursachen nicht, nur die Wahrscheinlichkeit des Eintretens lässt sich reduzieren.

4.3 Das Wissen der Community nutzen

Eine Open-Source-Lösung hat darüber hinaus einen ganz entscheidenden Vorteil gegenüber einer verborgenen, proprietären Technologie: Sie ist – auch hinsichtlich der Sicherheit – validiert durch die vielen Angehörigen der Community. Denn die meisten User profitieren nicht nur von der Gratisnutzung, sondern spielen ihre Erfahrungen, Fehlerberichte und Optimierungsvorschläge zurück, was allen Beteiligten zugutekommt. Man greift zudem auf das Fachwissen ganz vieler Experten und nicht nur auf das eigene und das der Kollegen zurück.

Open Source Software – Katalysator für Innovationen

Open Source Software beschleunigt Innovationen – innerhalb und außerhalb eines Unternehmens: Schließlich kann jeder Entwickler mit den Programmen kostenfrei und unkompliziert arbeiten, sie weiterentwickeln, Ideen ausprobieren und wieder verwerfen bzw. ihre Praxistauglichkeit durch die Community testen lassen.

Ein Beispiel dafür, dass sich Open Source bereits für Object Storage ausgezahlt hat, ist OpenStack. OpenStack erhält im Umfeld der Initiative zu mehr Datensouveränität – GAIA-X – einiges an Aufmerksamkeit. Das Open-Source-System enthält unter anderem die Komponenten „Swift“ und „Glance“. Swift dient dazu, eine große Anzahl unstrukturierter Daten mit einer einfachen API zu speichern bzw. abzurufen. Glance mit seiner RESTful API ist dafür da, um VM-Image-Metadaten zu verarbeiten, um Bilder virtueller Maschinen zu erkennen, zu registrieren und abzurufen. Datensouveränität – das heißt nicht nur mehr Kontrolle über Daten, sondern auch ein harmonisiertes Sicherheitsniveau sowie die Austauschbarkeit bei Migration von Dienstleister zu Dienstleister. Anbieter wie IONOS cloud unterstützen die Kompatibilität zu GAIA-X. Sie arbeiten aktiv an der Gestaltung der notwendigen technischen Umgebungen und liefern somit einen Erfahrungsschatz mit, der das Handling von Object Storage noch weiter abzusichern vermag und Nutzen für die Open Source Community stiftet. Gemeinsam sicher speichern - so die Devise.

5 Fazit

- Cloud und deren Storage-Möglichkeiten sind sicher, wenn man Sorgfalt walten lässt und mit den richtigen Dienstleistern arbeitet.
- Sicherheitsprobleme lassen sich weitgehend vermeiden.
- Die wichtigsten Maßnahmen sind:
  - Die Berechtigungen sollte man auf dem voreingestellten privaten Zugriff belassen.
  - Beim Erweitern von Berechtigungen ist eine möglichst restriktive Vorgehensweise ratsam.
  - Aller möglichen Szenarien sind mit anderen User Accounts zu testen.
  - Die Permissions von Buckets und Objekten sollten möglichst unabhängig voneinander sein.
  - Sichtbarkeit in gemeinsam genutzten Bereichen ist zu prüfen. Bucket- und Objektnamen können bereits schützenswerte Informationen enthalten, z. B. ‚Kündigung_Mitarbeiter_XYZ.pdf'.
  - Unternehmen müssen zudem berücksichtigen, dass User wieder verschwinden, etwa durch den Weggang eines Mitarbeiters.

Über IONOS

IONOS ist mit mehr als acht Millionen Kundenverträgen der führende europäische Anbieter von Cloud-Infrastruktur, Cloud-Services und Hosting-Dienstleistungen.

Das Produktportfolio bietet alles, was Unternehmen benötigen, um in der Cloud erfolgreich zu sein: von Domains über klassische Websites und Do-It-Yourself-Lösungen, Online-Marketing-Tools bis hin zu vollwertigen Servern und einer IaaS-Lösung. Das Angebot richtet sich an Freiberufler, Gewerbetreibende und Konsumenten sowie an Unternehmenskunden mit komplexen IT-Anforderungen.

IONOS cloud ist die europäische Cloud-Alternative von IONOS. Unser Produktportfolio umfasst mit der Cloud Compute Engine eine IaaS Compute Engine mit eigenem Code Stack für Virtualisierung, Managed Kubernetes für Container-Anwendungen, eine Private Cloud powered by VMware sowie S3 Object Storage. Mit unserem Angebot bieten wir etablierten mittelständischen und großen Unternehmen, regulierten Industrien, der Digitalwirtschaft und dem öffentlichen Sektor alle notwendigen Dienste und Services um in und mit der Cloud erfolgreich zu sein.

IONOS entstand 2018 aus dem Zusammenschluss von 1&1 Internet und dem Berliner IaaS-Anbieter ProfitBricks. 1&1 IONOS ist Teil der börsennotierten United Internet AG (ISIN DE0005089031). Zur 1&1 IONOS Markenfamilie gehören STRATO, Arsys,Fasthosts, home.pl, InterNetX, SEDO, United Domains und World4You.

Weitere Informationen unter www.ionos.cloud

Quellen- und Abbildungsverzeichnis

1. Achim Berg, Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.; Michael Niemeier, Bundesamt für Verfassungsschutz: „Wirtschaftsschutz in der digitalen Welt“, 6. November 2019, veröffentlicht unter https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019.pdf.
2. Matthias Janson, Statista GmbH: „2020 überholt die Cloud lokale Speichermedien“, 01. November 2019, veröffentlicht unter https://de.statista.com/infografik/18231/cloud-vs-lokaler-speicher/.
3. Palo Alto Networks, Inc., Unit 42: „Cloudy with a Chance of Entropy“; veröffentlicht auf https://unit42.paloaltonetworks.com/cloudy-with-a-chance-of-entropy/.
4. Palo Alto Networks, Inc., Unit 42: „Cloud Threat Report – Key findings and predictions for 2020“; veröffentlicht auf https://start.paloaltonetworks.com/unit-42-cloud-threat-report.

Impressum

1&1 IONOS SE
Elgendorfer Str. 57
56410 Montabaur, Germany

IONOS cloud Kontakt

Telefon +49 30 57700 850
Telefax +49 30 57700 8598

E-Mail info@cloud.ionos.de
Website https://www.ionos.cloud

Vorstand

Hüseyin Dogan, Dr. Martin Endreß, Claudia Frese, Hans-Henning Kettler, Arthur Mai, Matthias Steinberg, Achim Weiß

Aufsichtsratsvorsitzender

Markus Kadelke

Handelsregister

1&1 IONOS SE: Amtsgericht Montabaur / HRB 24498

Umsatzsteuer-IdentNummer

1&1 IONOS SE: DE815563912

Copyright

IONOS