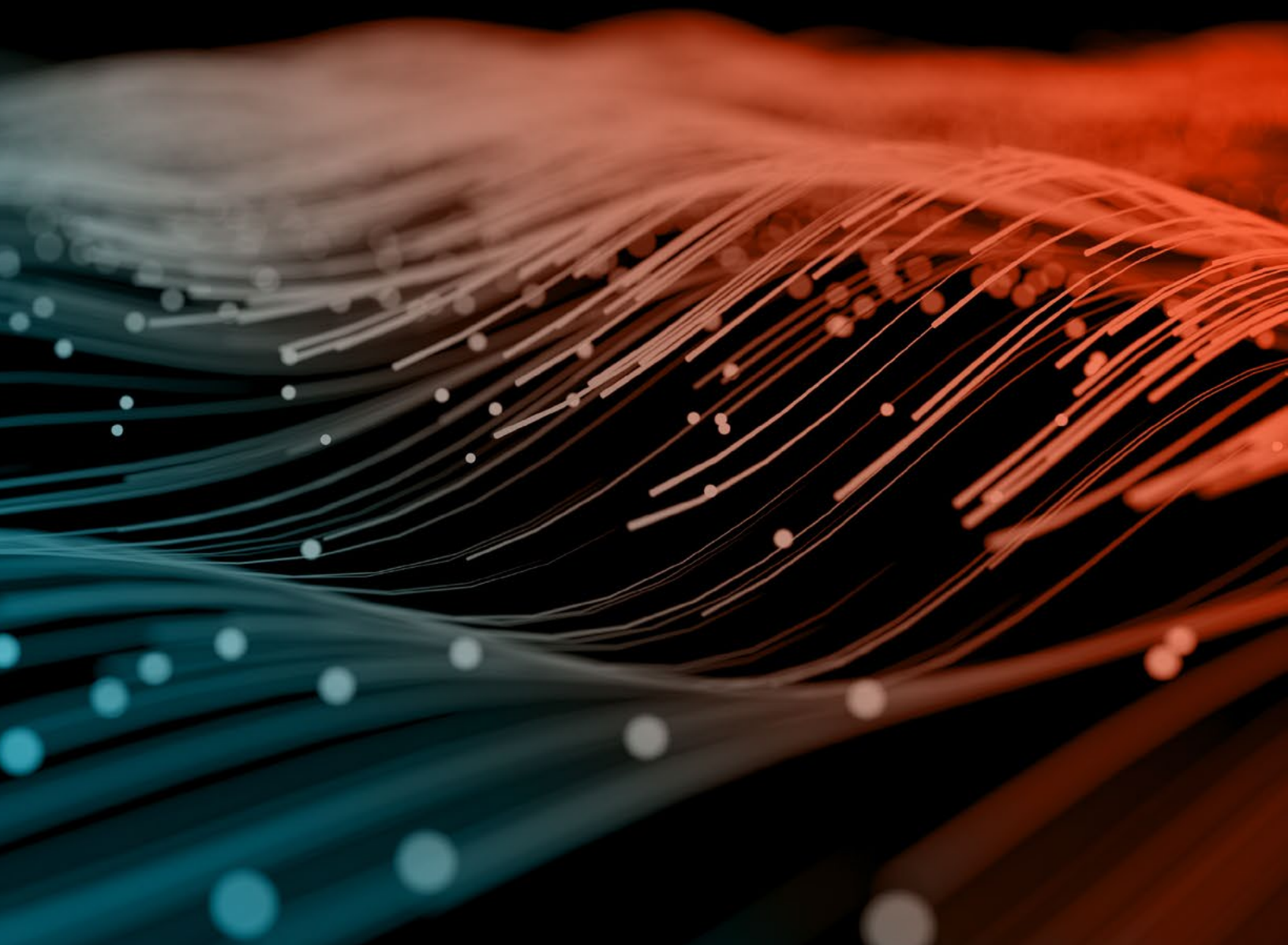
PRISMA CLOUD | UNIT 42 BY PALO ALTO NETWORKS

CLOUD THREAT REPORT
1. Jahreshälfte 2021

Das COVID-19-Dilemma: Risiko und Chance für die Cloud-Sicherheit



Inhaltsverzeichnis

Vorwort

Zu Beginn der COVID-19-Pandemie stieg die Nachfrage nach Cloud-Services schnell an. Innerhalb weniger Monate kletterte der Anteil der mobilen Arbeiter von 20 Prozent auf 71 Prozent.[1] Darüber hinaus erhöhten Unternehmen ihre Cloud-Ausgaben im dritten Quartal 2020 (Juli–September) sprunghaft um 28 Prozent gegenüber dem gleichen Quartal 2019.[2] Dieser Zeitraum ist aussagekräftig, da die Weltgesundheitsorganisation (WHO) COVID-19 im März 2020 zur Pandemie erklärt hat. Mit der Zunahme des mobilen Arbeitens beschleunigten Unternehmen ihre Cloud-Migrationspläne, mit einem erheblichen Anstieg im dritten Quartal 2020 im Vergleich zum Vorjahr.

Anhand von Daten von unseren weltweiten Sensoren erkannten unsere hoch qualifizierten Cloud-Bedrohungsforscher **eine Korrelation zwischen den gestiegenen Cloud-Ausgaben aufgrund von COVID-19 und der Anzahl der Sicherheitsvorfälle**.[3] Unternehmen weltweit haben ihre Cloud-Workloads um mehr als 20 Prozent erhöht (von Dezember 2019 bis Juni 2020), was zu einer explosionsartigen Zunahme an Sicherheitsvorfällen führte. Unsere Untersuchungen zeigen, dass Cloud-Sicherheitsprogramme in Unternehmen hinsichtlich der Automatisierung von Sicherheitsmaßnahmen (d. h. DevSecOps und Shift Left) weltweit noch in den Kinderschuhen stecken. All dies lässt uns folgern, dass **schnelle Cloud-Skalierung und Komplexität ohne automatisierte Sicherheitsmaßnahmen, die in die gesamte Entwicklungspipeline integriert sind, eine gefährliche Kombination** sind. Beispielsweise haben wir in einer früheren Untersuchung festgestellt, dass 65 Prozent der öffentlich bekannt gewordenen Sicherheitsvorfälle in der Cloud auf Fehlkonfigurationen seitens des Kunden zurückzuführen sind. Dies sind die Auswirkungen auf Unternehmen, die in der Cloud in großem Umfang und ohne automatisierte Sicherheitsmaßnahmen arbeiten.

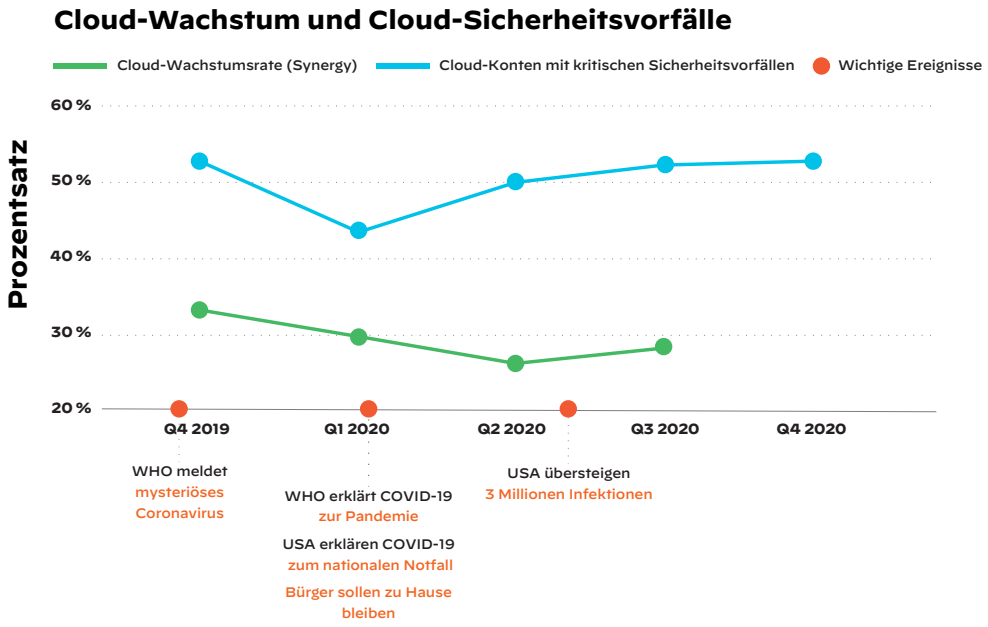


Abbildung 1: Zunehmende Cloud-Nutzung und Sicherheitsvorfälle

Lesen Sie in diesem Bericht, wie sich die neuesten weltweiten Cloud-Bedrohungen auf Ihr Unternehmen auswirken können und warum die Konzentration auf eine zentrale Sicherheitsplattform inklusive einheitlicher Standards Ihr Cloud-Sicherheitsprogramm entscheidend voranbringen kann.

Matthew Chiodi
Chief Security Officer, Public Cloud, Palo Alto Networks

1. „How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work", Pew Research Center, 9. Dezember 2020, https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work.
2. „COVID-19 Boosts Cloud Service Spending by $1.5 Billion in the Third Quarter", Synergy Research Group, 5. Dezember 2020, https://www.srgresearch.com/articles/covid-19-boosts-cloud-service-spending-15-billion-third-quarter.
3. Sicherheitsvorfälle sind definiert als Ereignisse, die Verstöße gegen Sicherheitsrichtlinien verursachen und sensible Daten gefährden.

Kurzfassung

Um die weltweiten Auswirkungen von COVID-19 auf die Unternehmenssicherheit zu verstehen, hat das Cloud Threat Intelligence Team Unit 42 Daten von Hunderten von Cloud-Konten auf der ganzen Welt für Oktober 2019 bis Februar 2021 (vor und nach dem Ausbruch der Pandemie) analysiert. **Unseren Forschungsergebnissen zufolge nahm die Anzahl der Sicherheitsvorfälle in der Cloud im zweiten Quartal 2020 – von April bis Juni – um ganze 188 Prozent zu. Wir stellten fest, dass sich viele Unternehmen nach einer mitunter überstürzten Migration ihrer Workloads in die Cloud angesichts der Pandemie Monate später damit abmühten, die Cloud-Sicherheit zu automatisieren und Cloud-Sicherheitslücken zu bekämpfen.** Obwohl Infrastructure-as-Code (IaC) DevOps- und Sicherheitsteams eine planbare Möglichkeit zur Durchsetzung von Sicherheitsstandards bietet, ist diese leistungsstarke Methode noch immer nicht weit verbreitet.

Dieser Bericht geht im Detail auf die Auswirkungen von COVID-19 auf die Bedrohungslandschaft in der Cloud ein und erläutert, welche Cybergefahren in bestimmten Regionen und Branchen am häufigsten beobachtet wurden. Außerdem zeigt der Bericht praktische Schritte auf, mit denen Unternehmen das Sicherheitsrisiko für ihre Cloud-Workloads reduzieren können.

Starker Anstieg der Sicherheitsvorfälle in COVID-19-kritischen Branchen

Unternehmen verlagerten nach Ausbruch der Pandemie umfangreiche Workloads in die Cloud, und die Anzahl der Sicherheitsvorfälle in der Cloud stieg erheblich. Insbesondere **stieg die Anzahl der Cloud-Sicherheitsvorfälle im Einzelhandel, in der Fertigung und in Behörden um 402 Prozent, 230 Prozent bzw. 205 Prozent**. Dieser Trend ist nicht überraschend, da die Pandemie diesen Branchen am meisten Anpassung und Skalierung abverlangt – Einzelhändlern für den Grundbedarf, Fertigung und Behörden für COVID-19-Hilfsgüter bzw. -Hilfsmaßnahmen.

Branchen, die bei der Bekämpfung der Pandemie eine entscheidende Rolle spielen, haben Schwierigkeiten, ihre Workloads in der Cloud zu schützen. Dies zeigt, wie gefährlich es ist, zu wenig in die Cloud-Sicherheit zu investieren. Die Zunahme an Cloud-Sicherheitsvorfällen macht deutlich, dass die Cloud Unternehmen zwar schnell mehr mobiles Arbeiten ermöglicht, dass aber automatisierte Sicherheitsmaßnahmen im Zusammenhang mit DevOps und CI/CD-Pipelines (Continuous Integration/Continuous Delivery) oft hinter dieser Entwicklung zurückbleiben.

Weniger Cryptojacking in der Cloud

Während der Hochphase der Pandemie gewannen Cryptowährungen wie Bitcoin (BTC), Ethereum (ETH) und Monero (XMR) an Beliebtheit und Marktwert. Trotzdem ist Cryptojacking rückläufig: Von Dezember 2020 bis Februar 2021 zeigten nur 17 Prozent der Unternehmen mit Cloud-Infrastruktur Anzeichen solcher Angriffe, gegenüber 23 Prozent von Juli bis September 2020. **Dies ist der erste verzeichnete Rückgang, seit Unit 42 im Jahr 2018 begann, Cryptojacking-Trends zu verfolgen.** Unternehmen scheinen Cryptojacking stärker proaktiv abzuwehren. Effektiv möglich ist dies durch einen Schutz der Workload-Laufzeitumgebung, der es Angreifern erschwert, bösartige Cryptomining-Software unerkannt in Cloud-Umgebungen von Unternehmen auszuführen.

Sensible Daten in der Cloud sind weiterhin öffentlich zugänglich

Unsere Ergebnisse zeigen, dass 30 Prozent der Unternehmen sensible Inhalte ungeschützt im Internet zugänglich machen, wie personenbezogene Daten, geistiges Eigentum sowie Patienten- und Finanzdaten. Jeder, der die URLs kennt oder erraten kann, kann auf diese Daten zugreifen. Wenn solche Daten ungeschützt über das Internet zugänglich sind, bestehen für das Unternehmen erhebliche Risiken in Bezug auf unbefugte Zugriffe und Verstöße gegen gesetzliche Vorschriften. Das Ausmaß der Gefährdung deutet darauf hin, dass Unternehmen immer noch Schwierigkeiten haben, angemessene Zugriffskontrollen für die Hunderte von Datenspeicher-Buckets umzusetzen, die sie potenziell in der Cloud betreiben, zumal wenn diese Buckets über mehrere Cloud-Anbieter und -Konten verteilt sind.

01

Evidenzbasierte Erkenntnisse

Wichtigste Cloud-Sicherheitsvorfälle im Zusammenhang mit COVID-19

Die Untersuchungen von Unit 42 zeigen einen erheblichen Anstieg verschiedenster Sicherheitsrisiken während der COVID-19-Pandemie. Die Risiken reichten von unverschlüsselten Cloud-Daten über öffentlich zugängliche Cloud-Ressourcen bis hin zu unsicheren Portkonfigurationen und mehr. Abbildung 2 zeigt über ein Dutzend Kategorien von Sicherheitsvorfällen, deren Häufigkeit erheblich zugenommen hat.

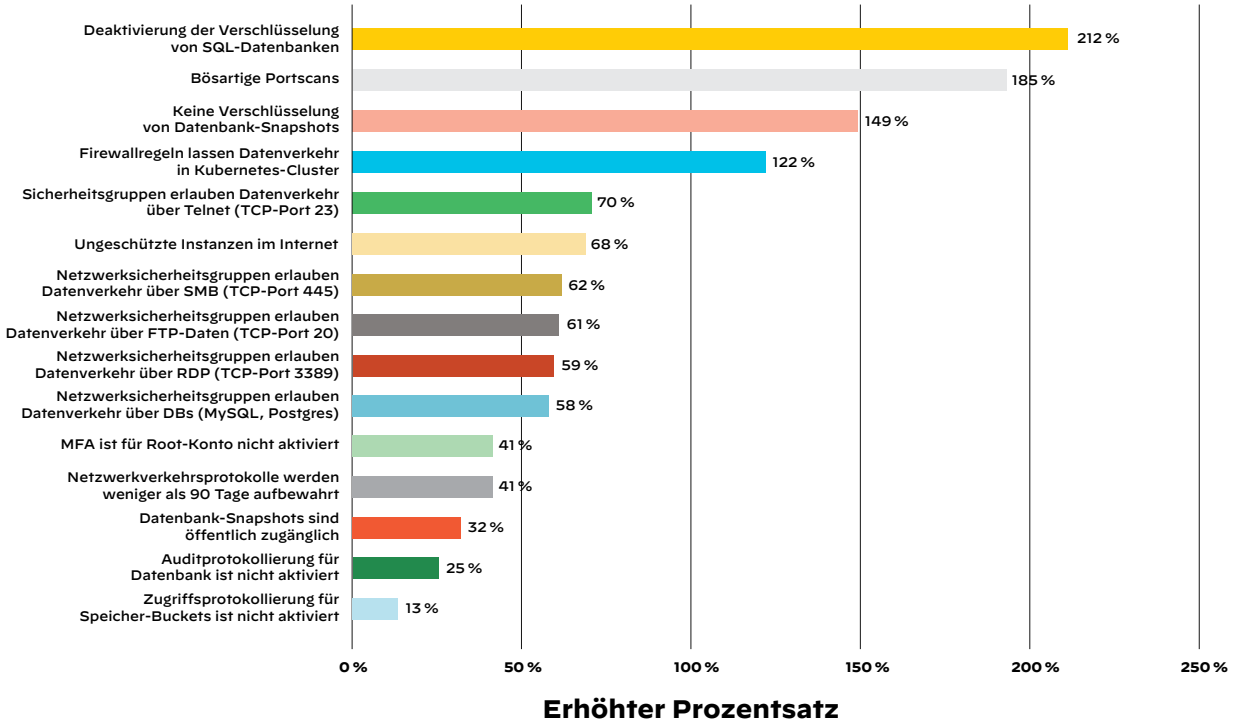


Abbildung 2: Sicherheitsvorfälle mit den größten Zunahmen während der Pandemie

Insgesamt **unterstreichen diese Vorfälle, dass die meisten Unternehmen nicht in der Lage sind, ihre Cloud-Governance und ihre Sicherheitsautomatisierung im gleichen Maße zu skalieren wie ihre Cloud-Workloads**. Viele dieser Fehlkonfigurationen können mithilfe von IaC-Vorlagen (Infrastructure-as-Code) behoben werden. Wie wir in früheren Berichten festgestellt haben, helfen IaC-Vorlagen, wenn sie konsequent auf häufige Sicherheitsschwachstellen überprüft werden, die Cloud-Infrastruktur von der Entwicklung bis zur Produktion zu sichern.

So kann beispielsweise die fehlende Verschlüsselung von SQL- und relationalen Datenbanken (z. B. Microsoft Azure® SQL Database) – eine der Sicherheitslücken, deren Häufigkeit am stärksten zugenommen hat – durch eine automatische Überprüfung von Cloud-Umgebungen auf Anzeichen von Fehlkonfigurationen leicht erkannt und korrigiert werden. Auch wenn Portscanning keine neue Bedrohung ist, deutet ihr vermehrtes Auftreten während der Pandemie darauf hin, dass Angreifer aktiv nach Schwachstellen suchen, die durch ineffektive Cloud-Governance entstehen.

Unzureichende Governance und Sicherheitsautomatisierung sind keine neuen Probleme. Obwohl die Häufigkeit von Benachrichtigungen im Zusammenhang mit Cloud-Sicherheitsvorfällen verschiedener Art im letzten Jahr zugenommen hat, sind unsere Ergebnisse bezüglich der häufigsten Arten von Vorfällen weitgehend mit denen unserer früheren Berichte vergleichbar.

Dies deutet darauf hin, dass Unternehmen, auch wenn sie im vergangenen Jahr mehr Workloads in die Cloud verlagert haben, weiterhin nicht gegen schwere Sicherheitsfehler und -mängel gefeit sind. So manche dieser Fehler können durch eine effektive Nutzung von IaC-Vorlagen vermieden werden. Viele Teams verwenden bereits IaC-Vorlagen, allerdings nicht so effektiv wie möglich. Die meisten dieser Vorlagen werden in einem einfachen dreistufigen Prozess erstellt: Entwerfen, Codieren und Bereitstellen. Was DevOps- und Sicherheitsteams in Schwierigkeiten bringt, ist das Fehlen von automatisierten Sicherheitsüberprüfungen. Genau wie Anwendungscode müssen IaC-Vorlagen bei der Erstellung und bei jeder Aktualisierung auf Sicherheitsprobleme überprüft werden.

Unsere Untersuchungen zeigen jedoch, dass Teams während der Hochphase der Pandemie entweder IaC gar nicht verwendeten oder es einfach versäumten, auf häufige Sicherheitslücken zu prüfen. So sind ihnen Fehler unterlaufen wie die fehlende Verschlüsselung potenziell sensibler Daten oder die fehlende Aktivierung der Protokollierung, die für die Sicherheitsüberwachung und -prüfung in Cloud-Umgebungen von entscheidender Bedeutung ist.

Auswirkungen von COVID-19 auf die Cloud-Sicherheit nach Region

Die Auswirkungen der Pandemie auf die Zunahme der Cloud-Nutzung waren weltweit in allen Regionen zu beobachten, aber wie Abbildung 3 zeigt, waren sie in einigen Regionen stärker als in anderen.

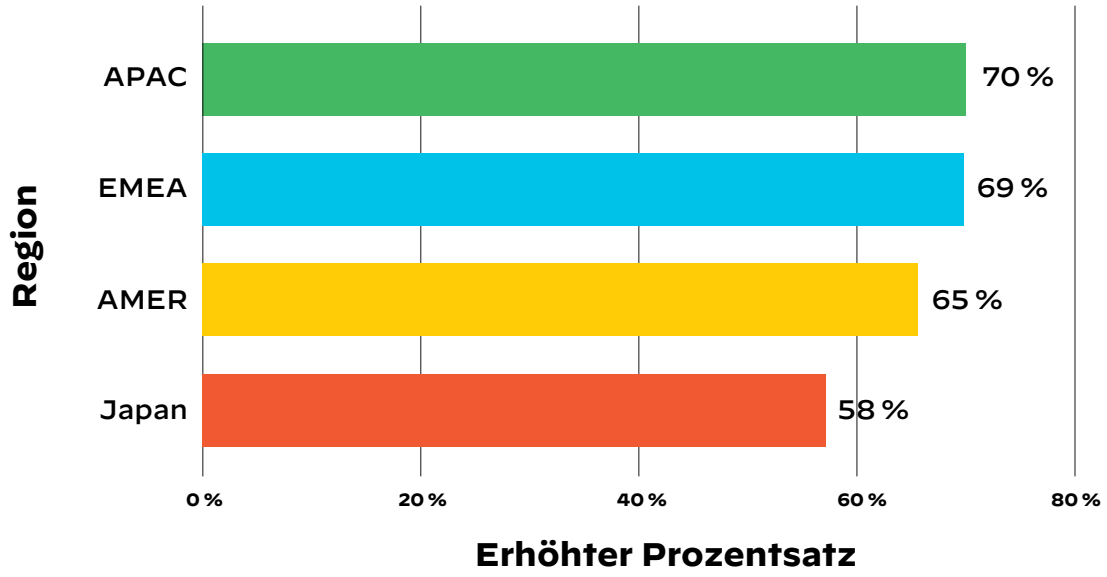


Abbildung 3: Zunahme der Cloud-Workloads nach Region

Insgesamt war der Wechsel in die Cloud in Japan während der Pandemie langsamer als in anderen Ländern. Daher wiesen nur 32 Prozent der japanischen Unternehmen unsichere Konfigurationen auf, die für mindestens eine ihrer in der Cloud gehosteten virtuellen Maschinen (VMs) den gesamten Netzwerkverkehr (TCP/UDP auf jedem Port) zuließen, und nur 39 Prozent hatten Port 22 (SSH) in mindestens einem ihrer in der Cloud gehosteten SSH-Services geöffnet.

Im Vergleich dazu ließen weltweit 60 Prozent der Unternehmen für ihre Cloud-Plattformen den gesamten Netzwerkverkehr zu, und 58 Prozent hatten Port 22 geöffnet.

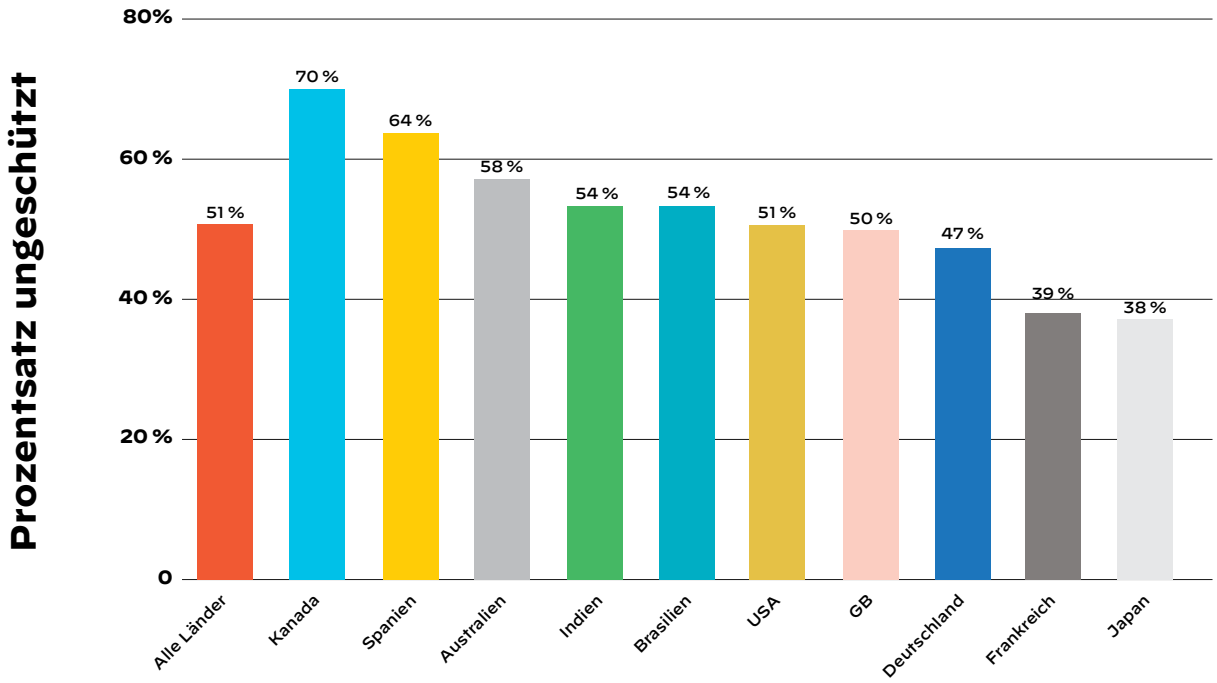


Abbildung 4: Prozentsatz der Unternehmen mit ungeschütztem RDP nach Land

Auch Windows Remote Desktop Protocol (RDP, Port 3389) war je nach Region sehr unterschiedlich oft ungeschützt (siehe Abbildung 4). Diese Schwachstelle zu erkennen, ist wichtig, da RDP einer der beliebtesten Angriffsvektoren ist. Angreifer können über geöffnete RDP-Ports in Unternehmensnetzwerke eindringen, um den Betrieb zu stören oder sensible Daten zu stehlen. Unternehmen in Kanada hatten in diesem Bereich am häufigsten Probleme: 70 Prozent von ihnen ließen RDP ungeschützt.

Ein Vergleich der Zunahme an Cloud-Workloads nach Region mit der ungeschützten Zugänglichkeit von RDP in den einzelnen Ländern zeigt ein Muster im Zusammenhang mit COVID-19. Die Forscher von Unit 42 fanden eine direkte Korrelation mit vermehrten Sicherheitsvorfällen. Im Durchschnitt über alle großen Cloud-Anbieter stieg die ungeschützte Zugänglichkeit von RDP um 27 Prozent.

Auch hier sind ungesicherte kritische Ports ein Fehler mit potenziell schwerwiegenden geschäftlichen Folgen. Dieser Fehler kann jedoch mit einer Kombination aus sicherem IaC und kontinuierlicher Sicherheit über eine zentrale Sicherheitsplattform verhindert werden.

Auswirkungen von COVID-19 auf die Cloud-Sicherheit nach Branche

Der Umfang der Cloud-Workloads nahm in fast allen Branchen zu. Die einzige Ausnahme bildete der Energiesektor, was wahrscheinlich auf die schwache Nachfrage und den Rückgang der Öl- und Gasproduktion während der Pandemie zurückzuführen ist. Am meisten stieg die Cloud-Nutzung in Behörden, der chemischen Industrie, der Pharmaindustrie und den Biowissenschaften. Dies ist wahrscheinlich auf ihre arbeitsintensive Reaktion auf die Pandemie zurückzuführen.

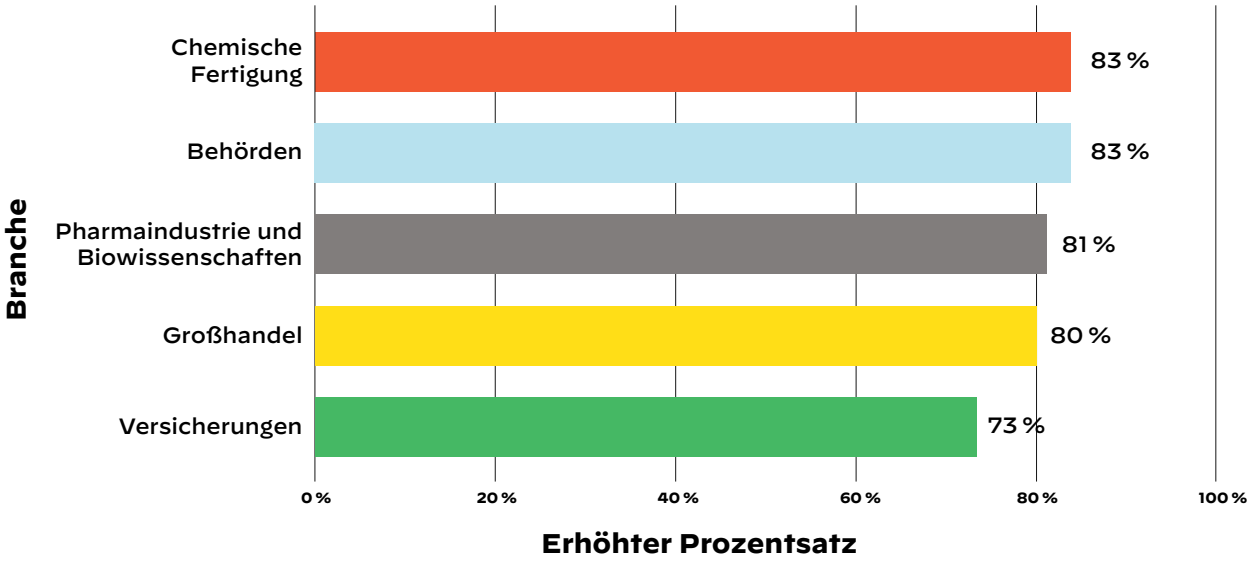


Abbildung 5: Prozentualer Anteil der Unternehmen mit gestiegenen Cloud-Workloads nach Branche

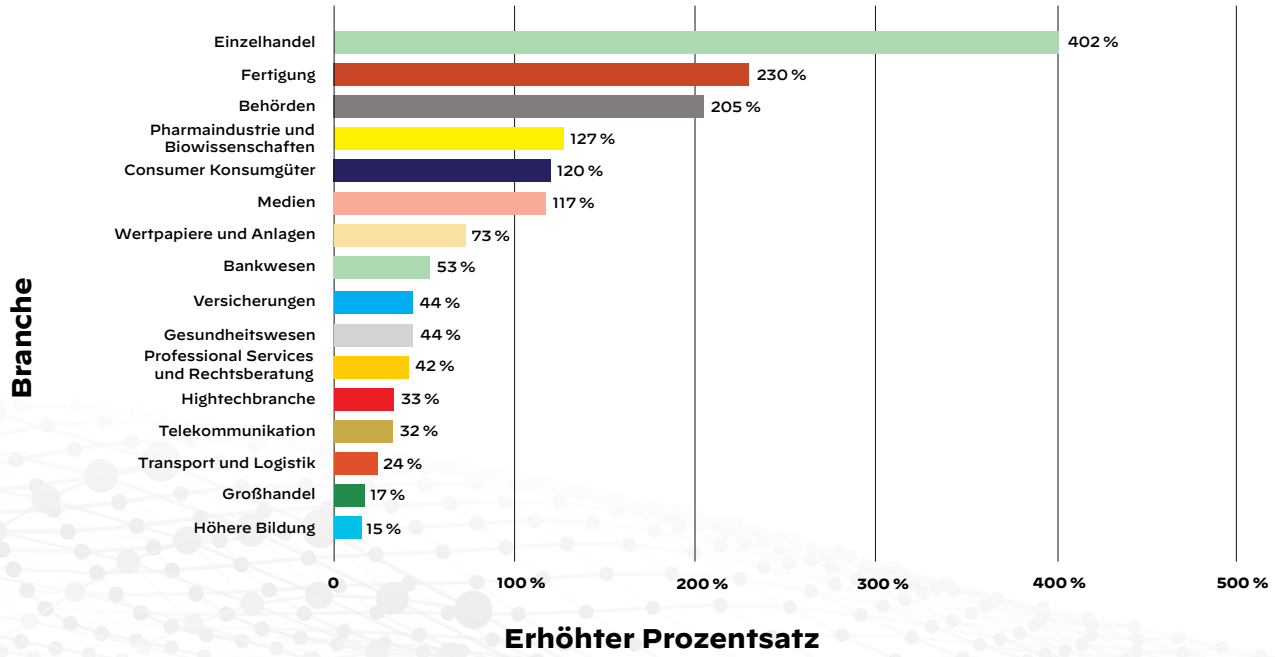


Abbildung 6: Prozentualer Anstieg der Sicherheitsvorfälle nach Branche

Hinweis: Branchen mit zu kleinen Stichproben sind in den Zahlen nicht enthalten.

Unsere Untersuchungen zeigen, dass bei einem plötzlichen Anstieg der Cloud-Workloads eines Unternehmens die Anzahl der Sicherheitsvorfälle drastisch ansteigt – oft so sehr, dass DevOps- und Sicherheitsteams überfordert sind. Beispielsweise stieg die Anzahl der Sicherheitsvorfälle im Einzelhandel, in der Fertigung und in Behörden um 402 Prozent, 230 Prozent bzw. 205 Prozent. Dieser Trend ist nicht überraschend, da die Pandemie diesen Branchen viel Anpassung und Skalierung abverlangt – Einzelhändlern für den Grundbedarf, Fertigung und Behörden für COVID-19-Hilfsgüter bzw. -Hilfsmaßnahmen. Diese Vorfälle vergrößerten die Angriffsflächen von Cloud-Umgebungen und erschwerten Sicherheitsaudits und forensische Bemühungen.

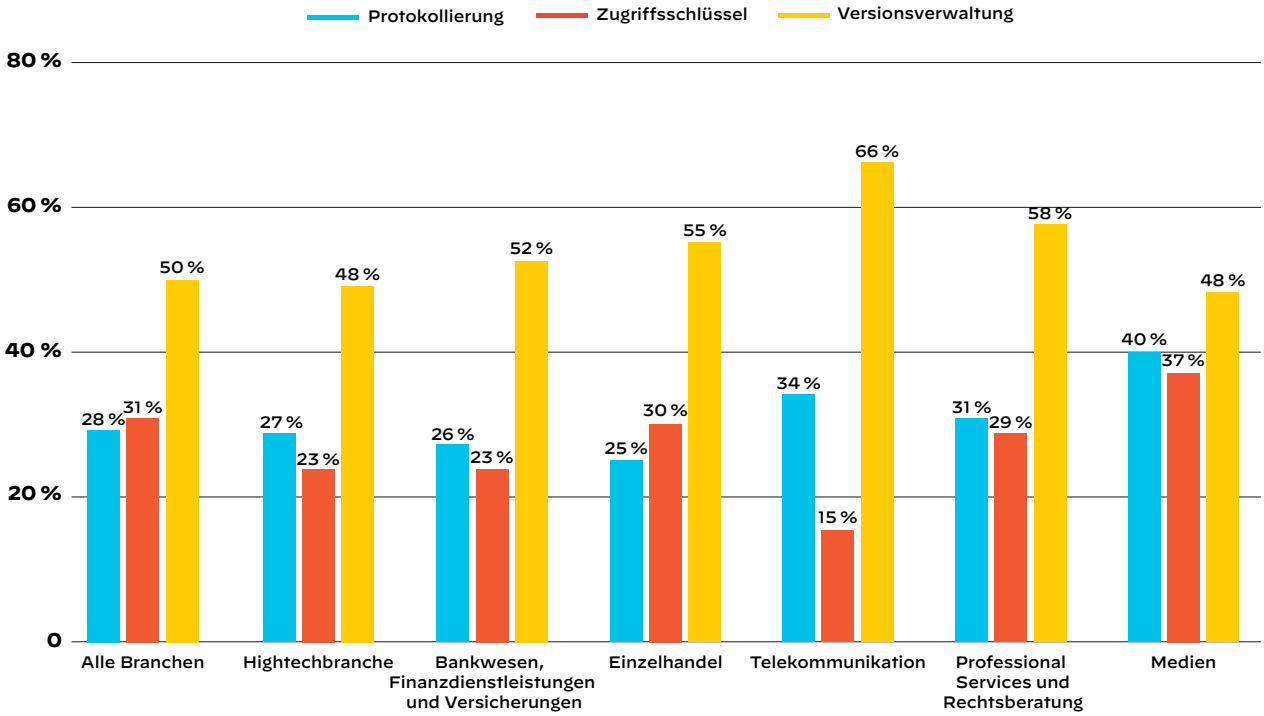


Abbildung 7: Prozentsatz der Unternehmen, die kritische Sicherheitsmaßnahmen nutzen, nach Branche

Dennoch war die Sicherheit in einigen Branchen höher als in anderen (siehe Abbildung 7). Beispielsweise nutzten 40 Prozent der Medienunternehmen weltweit eine Zugriffsprotokollierung für jeden ihrer Cloud-Speichercontainer. Im Einzelhandel war dies nur bei 25 Prozent der Unternehmen der Fall. Die Gründe dafür sind zurzeit nicht bekannt, aber die Forscher von Unit 42 gehen davon aus, dass Medienunternehmen meist sehr auf den Zugang zu Inhalten achten, zumal ihnen die Folgen des Sony Pictures-Hacks im Jahr 2014 bewusst sind.

Auch wurden in der Medienbranche die Zugangsschlüssel häufiger geändert: In 37 Prozent der Medienunternehmen waren die Zugangsschlüssel weniger als 90 Tage alt, aber nur in 15 Prozent der Telekommunikationsunternehmen. Auch hier gehen die Forscher von Unit 42 davon aus, dass Medienunternehmen das Zugriffsmanagement meist sehr ernst nehmen. Die Telekommunikationsbranche hingegen stand an zweiter Stelle bei den Protokollierungsmaßnahmen, aber an letzter Stelle bei der Schlüsselverwaltung, was darauf hindeutet, dass diese Branche die Überwachung wichtiger nimmt als die Zugriffskontrolle.

Die Versionskontrolle innerhalb von Cloud-Speichercontainern ist eine wichtige Sicherheitsmaßnahme, da sie darüber entscheidet, ob sich ein Unternehmen von erfolgreichen Angriffen auf Cloud-Speicher sowie von Dateibeschädigungsfehlern erholen kann. In der Telekommunikationsbranche hatten 66 Prozent der Unternehmen in allen ihren Cloud-Speichercontainern eine Versionskontrolle implementiert; das Schlusslicht bildeten die Medien- und die Hightechbranche mit jeweils nur 48 Prozent. Den Forschern von Unit 42 fiel auf, dass die Medien- und die Telekommunikationsbranche praktisch entgegengesetzte Sicherheitsmodelle verfolgen. Beide legen den Schwerpunkt auf Protokollierungs- und Überwachungsmaßnahmen, aber während die Medienbranche Zugriffsschlüssel bevorzugt, setzt die Telekommunikationsbranche auf Versionskontrollen. So sehr, wie Medienunternehmen darauf achten, den Zugang zu kontrollieren, achten Telekommunikationsunternehmen darauf, dass ihre Daten nicht kompromittiert werden.

COVID-19 und die Datensicherheit

Unternehmen bevorzugen Cloud-Speicherung aufgrund der hohen Zuverlässigkeit, Verfügbarkeit und Skalierbarkeit. Unsere Untersuchungen zeigen, dass 64 Prozent der Daten in der Cloud sensible Informationen enthalten (z. B. personenbezogene Daten, geistiges Eigentum, Patienten- und Finanzdaten). Von diesen 64 Prozent enthalten 69 Prozent personenbezogene Daten und 34 Prozent geistiges Eigentum (siehe Abbildung 8).

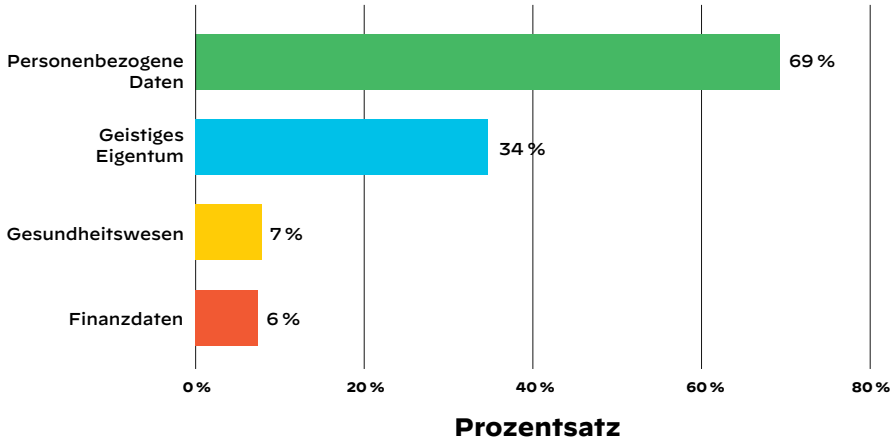


Abbildung 8: Häufigkeit von Datenarten unter den in Clouds gespeicherten sensiblen Daten

Während der Umfang der in der Cloud gespeicherten Daten zunahm, richteten viele Unternehmen keine angemessenen Sicherheitsmaßnahmen für diese Daten ein. Unsere Untersuchungen zeigen, dass die Cloud-Speicherressourcen von 35 Prozent der Unternehmen weltweit öffentlich über das Internet zugänglich sind. Auch wenn diese Konfiguration in bestimmten Fällen notwendig sein kann, ist sie in der Regel wahrscheinlich ein Fehler, der aufgrund mangelnder Sicherheitsüberwachung und -audits übersehen wurde.

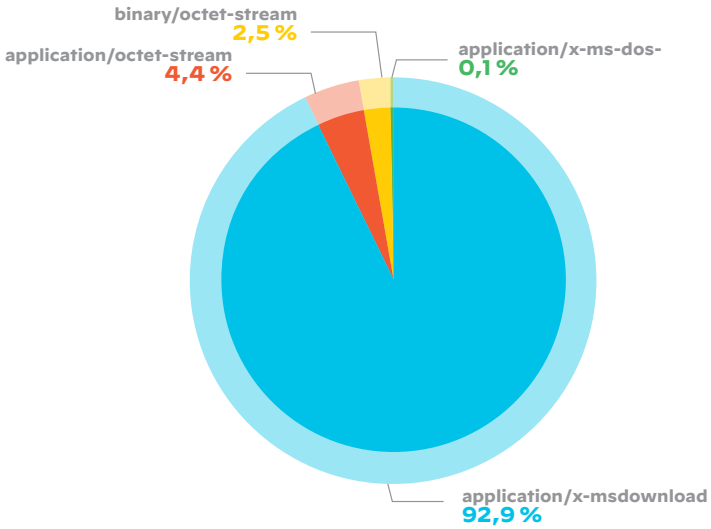


Abbildung 9: Malwarearten in Cloud-Speichern

Unternehmen mit öffentlich zugänglichen Cloud-Daten sind einem besonders hohen Risiko ausgesetzt, zumal weltweit 30 Prozent von ihnen dabei offenbar sensible Daten speichern. **Dieses Ergebnis ist schockierend, da jeder, der die richtigen URLs kennt, ohne Passwörter oder andere Authentifizierung auf die Daten zugreifen kann**. In den letzten Jahren gab es zahlreiche Vorfälle, bei denen Forscher oder Angreifer sensible Daten in Cloud-Speichern entdeckten, die versehentlich öffentlich zugänglich waren. So fanden Forscher von vpnMentor in ungeschützten Cloud-Speicherumgebungen personenbezogene Daten von mehr als 30.000 Personen, und Forscher von The Register fanden mehr als 500.000 vertrauliche Dateien, die zu Tausenden von Kunden gehörten.

Neben sensiblen Daten können Cloud-Speicher auch Malware enthalten. Forscher von Unit 42 stellten fest, dass 92,9 Prozent der Malware in Cloud-Speichern sich in ausführbaren Dateien (.exe) oder DLL-Dateien (.dll) befindet. Dieser Prozentsatz passt zu der Erkenntnis von VirusTotal, dass die meiste Malware auf Windows-Systeme abzielt und dass ausführbare Dateien das häufigste Übertragungsmedium sind.

Die gute Nachricht ist, dass wir Malware in weniger als 0,01 Prozent der Daten in Cloud-Speichern gefunden haben. Für diese 0,01 Prozent muss jedoch untersucht werden, wie die Malware in den Speicher gelangt ist und wer auf sie zugegriffen haben könnte.

02

Die Cloud, COVID-19 und Cryptowährungen

Auch wenn die Entwicklungen auf dem Cryptowährungsmarkt und die damit verbundenen Sicherheitsprobleme nicht ausschließlich mit der COVID-19-Pandemie in Verbindung gebracht werden können, zeigen unsere Untersuchungen interessante Verbindungen zwischen Cryptowährungen, der Cloud und den Auswirkungen von COVID-19.

Die Forscher von Unit 42 konzentrierten sich auf Daten im Zusammenhang mit Monero (XMR), einer Cryptowährung, die bei Hackern aufgrund ihrer hohen Anonymität und ihres einfachen Minings in der Cloud beliebt ist. Die Forschung fand von Dezember 2020 bis Februar 2021 statt.

Mining-Trends und Marktereignisse

Unsere Ergebnisse zeigen, dass die **Verbindungen mit bekannten XMR-Cryptomining-Pools in diesem Zeitraum um 65 Prozent zunahmen**, mit enormen Höhen und Tiefen in der Gesamtzahl der Verbindungen.

Besonders interessant war dabei, dass in drei Fällen die niedrigsten Anzahlen von Netzwerkverbindungen zugleich mit den höchsten Marktpreisen auftraten (siehe Abbildung 10). Dies könnte darauf hindeuten, dass Cryptomining-Akteure den Großteil ihres Minings während sinkender Kurse durchführen und es dann unterbrechen, um ihre Beute in Zeiten höherer Preise zu verkaufen. Bemerkenswert ist auch der anhaltende Rückgang der XMR-Netzwerkverbindungen vom 24. Dezember 2020 bis zum 3. Januar 2021, was darauf hindeutet, dass auch illegale Cryptomining-Projekte eine Weihnachtspause einlegen müssen.

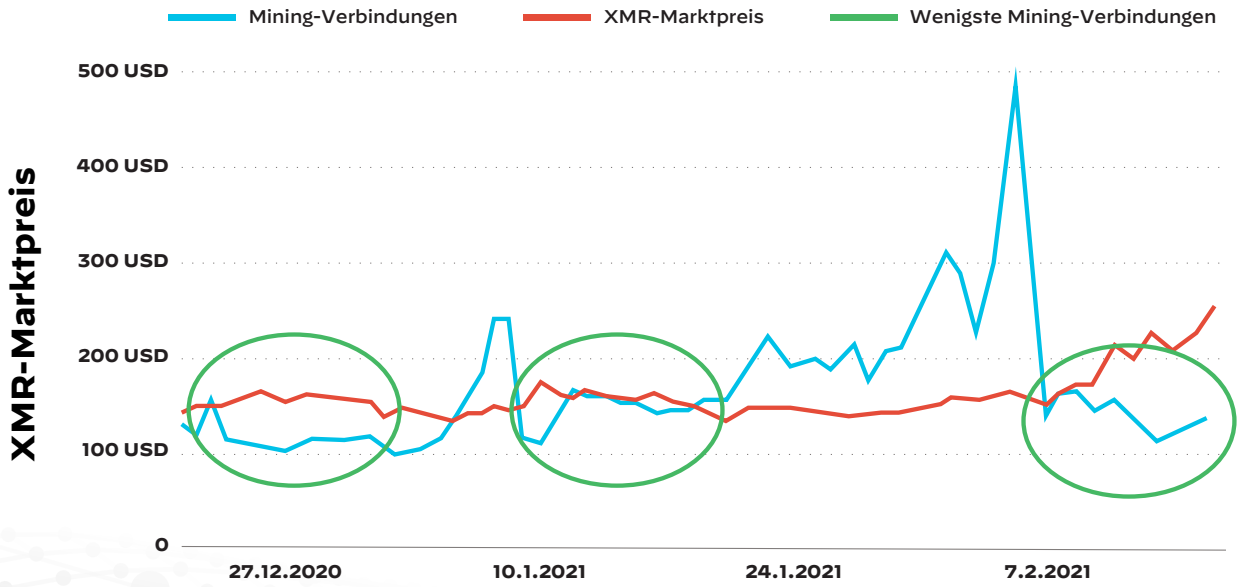


Abbildung 10: Vergleich von Cryptomining-Verbindungen und XMR-Preis

Die Auswirkungen der Pandemie auf das Mining

Forscher von Unit 42 haben eine klare Korrelation zwischen XMR-Mining-Aktivitäten und Ereignissen im Zusammenhang mit der Pandemie festgestellt. Abbildung 11 zeigt die Häufigkeit, mit der XMR-Mining-Pools Netzwerkverbindungen hergestellt haben, zusammen mit wichtigen Daten der Pandemie.

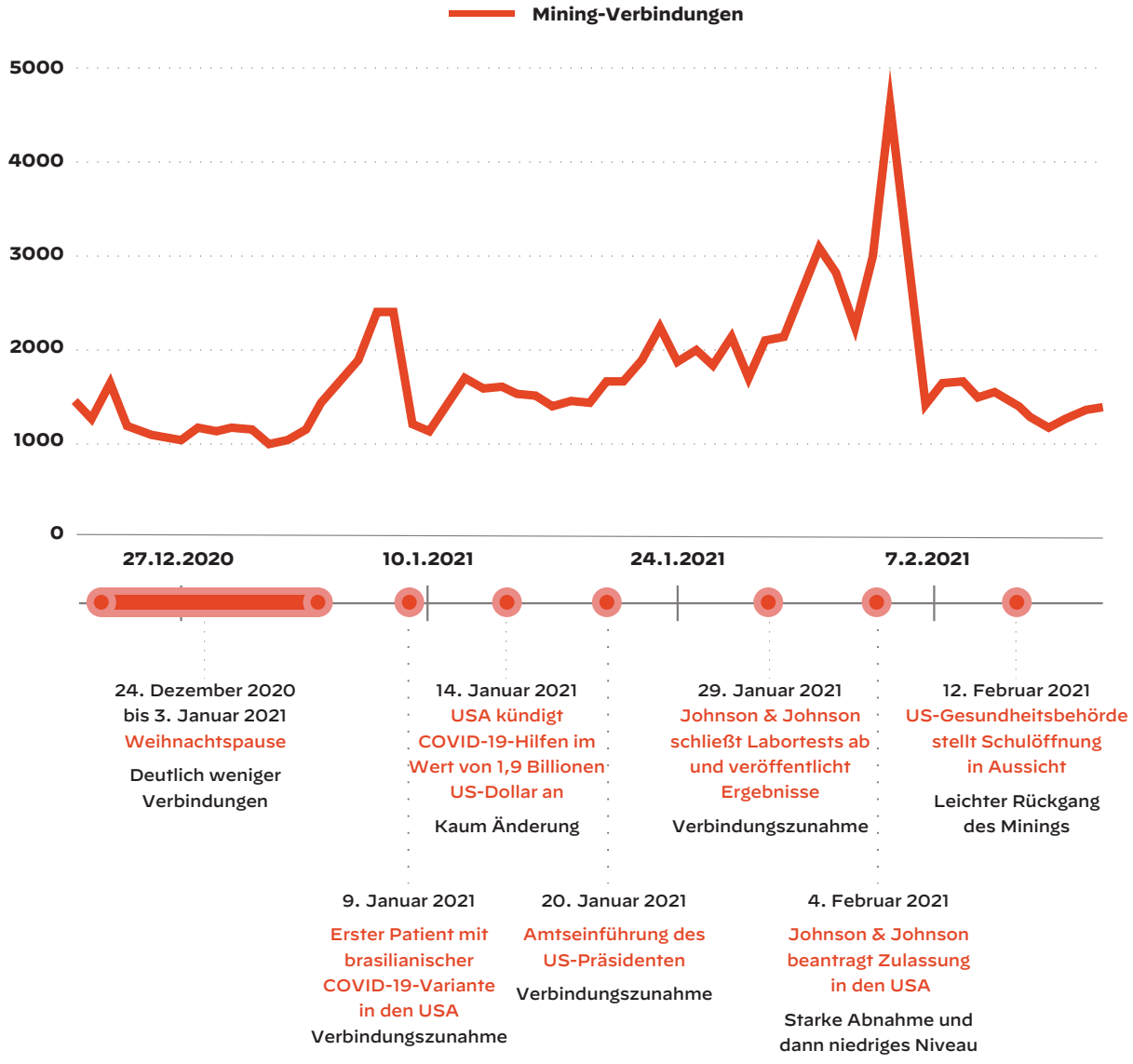


Abbildung 11: Mining-Pool-Verbindungen und wichtige Daten

Obwohl der vorhandene Datenumfang nicht für endgültige Schlussfolgerungen ausreicht, ist es wahrscheinlich, dass Ereignisse in Politik und öffentlicher Gesundheit einen deutlichen Einfluss auf böswillige Cryptomining-Operationen haben, zumindest für XMR.

Rückgang des Cryptojacking

Trotz erhöhter Mining-Aktivitäten ist das Cryptojacking (d. h. die unbefugte Nutzung von Infrastrukturen für Cryptomining) in der COVID-19-Zeit zurückgegangen. Weltweit wurden von Juli bis September 2020 laut unseren Ergebnissen 23 Prozent der Unternehmen mit Cloud-Workloads Opfer von Cryptojacking, im Vergleich zu nur 17 Prozent von Dezember 2020 bis Februar 2021. **Dies ist der erste verzeichnete Rückgang, seit wir im Jahr 2018 begonnen haben, Cryptojackingaktivitäten zu verfolgen**.

Auch wenn XMR die beliebteste Cryptowährung für Mining in der Cloud ist, haben andere Cryptowährungen einen größeren Marktanteil. Forscher von Unit 42 haben die Netzwerkverbindungen für Ethereum (ETH), Bitcoin (BTC), Litecoin (LTC) und Dash untersucht. Dabei beobachteten sie viel mehr Mining-Verbindungen für XMR als für jede der anderen Währungen. Auf diese zusammen entfielen nur durchschnittlich 1 Prozent so viele Netzwerkverbindungen wie auf XMR (siehe Abbildung 12).

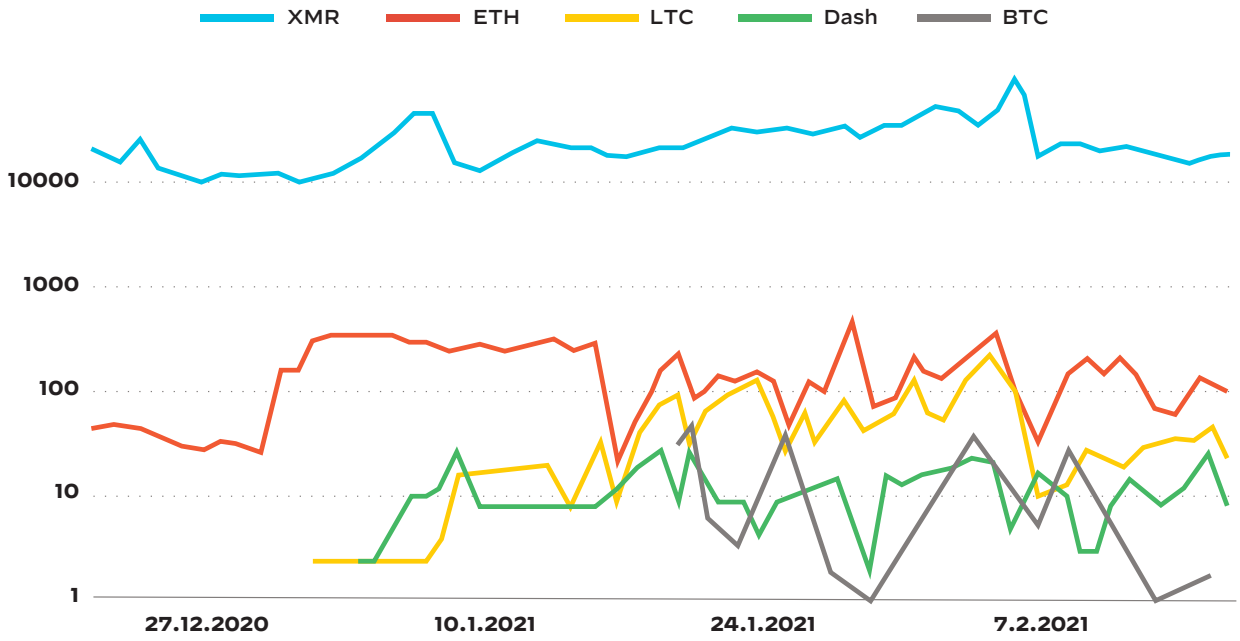


Abbildung 12: Mining-Verbindungen nach Cryptowährung

ETH, eine der beliebtesten Cryptowährungen, lag nach XMR an zweiter Stelle bei der Anzahl von Netzwerkverbindungen zu Währungs-Mining-Pools. Dies ist nicht unerwartet, da ETH von allen Cryptowährungen wohl am meisten Funktionalität bietet. Während das Mining von ETH mit CPU-basierter Verarbeitung nicht besonders effizient ist, bieten alle Cloud-Service-Provider (CSPs) VM-Instanzen mit Grafikprozessoren (GPUs) an, die für das Cryptomining deutlich effizienter sind als CPUs.

Für BTC, LTC und Dash wurden überraschenderweise jeweils Netzwerkverbindungen zu eigenen Mining-Pools beobachtet. Die Mining- und Proof-of-Work-Prozesse für Blockchainwährungen wie BTC, LTC und Dash sind arbeitsspeicherintensiver und sind nur mit spezieller Hardware rentabel, sogenannten ASIC-Minern (Application Specific Integrated Circuit). Aufgrund ihrer Ineffizienz für das cloudbasierte CPU/GPU-Mining und des negativen Kosten-Nutzen-Verhältnisses sollten alle Netzwerkverbindungen zu diesen Mining-Pools aus der Cloud-Infrastruktur von Unternehmen als höchst verdächtig betrachtet werden.

03

Schlussfolgerung und Empfehlungen

Die wichtigste Erkenntnis aus unseren Daten ist klar: **Unternehmen haben es versäumt, in die Cloud-Governance und in automatisierte Sicherheitsmaßnahmen zu investieren, die notwendig sind, damit ihre Workloads auch nach der Verlagerung in die Cloud sicher bleiben.** Damit haben sie sich schwerwiegende Geschäftsrisiken eingehandelt, indem sie etwa sensible Daten unverschlüsselt über das Internet verfügbar machen und Angriffe provozieren, indem sie unsichere Ports geöffnet lassen. Während die Cloud Threat Reports unserer Unit 42 im Jahr 2020 ähnliche Probleme aufzeigten, haben die zahlreichen Krisen, die durch die COVID-19-Pandemie ausgelöst wurden, die Situation noch schwieriger und umfangreicher gemacht.

Angesichts dieser Bedrohung müssen Unternehmen ein Cloud-Sicherheitsprogramm aufbauen, das alle Phasen des Softwareentwicklungszyklus gleichmäßig berücksichtigt. So können sie nicht nur am Markt erfolgreich sein, sondern auch nachhaltige Cloud-Sicherheitsprogramme einrichten, die sie hoch- und herunterskalieren können, ganz gleich, was für unvorhersehbare Ereignisse die Zukunft bringt.

Strategische Schwerpunktbereiche für die Cloud-Sicherheit

Insbesondere empfehlen die Forscher von Unit 42, sich auf bestimmte strategische Bereiche der Cloud-Sicherheit zu konzentrieren.

Verschaffen Sie sich ein umfassendes, detailliertes Bild der Cloud-Nutzung

Als ersten Schritt zu einfacherer Cloud-Sicherheit und Compliance sollten Sie sich ein umfassendes Bild der aktuellen Cloud-Nutzung Ihrer Entwickler und der Teams in den Geschäftsbereichen machen. Das bedeutet, dass Sie die Vorgänge in Ihren Cloud-Umgebungen bis hinunter zur API- und Workload-Ebene stets genau analysieren.

Implementieren Sie Kontrollmechanismen

Fragen Sie sich, welche Fehlkonfigurationen in Ihrer Umgebung nie vorkommen sollten. Ein Beispiel hierfür ist eine Datenbank, in die direkt aus dem Internet Befehle eingegeben werden können. Das ist eine der gefährlichsten Sicherheitslücken überhaupt, aber unsere Forscher haben sie in 28 Prozent der untersuchten Cloud-Umgebungen weltweit gefunden. Wenn Fehlkonfigurationen wie diese gefunden werden, sollten Ihre Sicherheitskontrollen sie automatisch korrigieren. Falls noch nicht geschehen, sollten Sie IaC-Vorlagen als zusätzliche Möglichkeit zur Durchsetzung von Sicherheitskontrollen im Rahmen des Shift Left in Erwägung ziehen. Überprüfen Sie diese Vorlagen unbedingt auf häufige Sicherheitsfehlkonfigurationen.

Führen Sie Standards ein und setzen Sie sie durch

Es ist extrem schwierig, etwas zu automatisieren, das nicht standardisiert wurde. In vielen Teams wird über die Automatisierung diskutiert, obwohl es noch gar keine Sicherheitsstandards gibt. Beginnen Sie nicht bei Null. Das Center for Internet Security (CIS) bietet Benchmarks für alle wichtigen Cloud-Plattformen. Sie sollten diese Standards mithilfe von IaC automatisieren und kodifizieren.

Ihre Sicherheitstechniker sollten programmieren können

Anders als in den meisten herkömmlichen Rechenzentren spielen APIs in Public-Cloud-Umgebungen eine wichtige Rolle. Für ein erfolgreiches Risikomanagement in der Cloud müssen Sicherheitsteams in der Lage sein, diese APIs zu nutzen, um die Sicherheit von Workloads in großem Umfang zu verwalten. Dafür braucht Ihr Sicherheitsteam Techniker, die sich mit der Programmierung und Automatisierung von Sicherheitsprozessen im Rahmen der CI/CD-Pipeline auskennen.

Integrieren Sie die Sicherheit in DevOps

Zeichnen Sie genau auf, wer wann welchen Code in welche Cloud-Umgebung(en) hochlädt. Wenn Sie das wissen, können Sie ermitteln, an welchem Punkt Ihrer CI/CD-Pipeline Sicherheitsprozesse und -tools implementiert werden sollten, um den Code effektiv zu schützen und die Entwickler möglichst wenig zu behindern. Beziehen Sie daher das DevOps-Team unbedingt von Anfang an in diesen Prozess ein. Minimieren Sie dann nach und nach den manuellen Anteil, indem Sie so viele Vorgänge wie möglich automatisieren.

Sind Sie in der Lage, die Bedrohungen in Ihrer Cloud zu erkennen?

Prisma Cloud analysiert jeden Monat mehr als 10 Milliarden Ereignisse. Diese Analysen zeigen immer wieder, dass Fehlkonfigurationen, laxes Verhalten und fehlende Richtlinien zu vielen Schwachstellen führen, die von Hackern und nicht identifizierten Bedrohungen ausgenutzt werden können. Durch die proaktive Erkennung von Sicherheits- und Compliancefehlkonfigurationen sowie die automatisierte Einleitung angemessener workflowbasierter Gegenmaßnahmen trägt Prisma Cloud dazu bei, dass Sie die Anforderungen Ihrer dynamischen Cloud-Workloads kontinuierlich und sicher erfüllen.

Methodik

Alle in diesem Bericht vorgestellten Untersuchungen basieren auf Daten, die von Oktober 2019 bis Februar 2021 erhoben wurden. Die Untersuchungen bezogen sich auf Unternehmen und Branchen weltweit, d. h. in Nord- und Südamerika, Europa, dem Nahen Osten und Afrika (EMEA) sowie Japan und Asien-Pazifik (JAPAC).

Prisma Cloud von Palo Alto Networks

Prisma® Cloud-Trenddaten nutzen mehrere Threat Intelligence-Quellen. Die Forscher von Unit 42 nutzten proprietäre Datenquellen, um Benachrichtigungs- und Ereignisdaten von Unternehmen zu sammeln. Diese Daten wurden anonymisiert und anschließend analysiert und mit den Analyseergebnissen in früheren Berichten über Cloud-Bedrohungen verglichen, um Trendinformationen zu erhalten.

WildFire von Palo Alto Networks

Der cloudbasierte Malwareschutzservice WildFire® kombiniert statische und dynamische Analysen mit innovativen maschinellen Lernverfahren und einer neuartigen Umgebung für die Baremetalanalyse in einem einzigartigen, mehrgleisigen Ansatz zur Erkennung auch bestens getarnter Bedrohungen.

AutoFocus von Palo Alto Networks

Der kontextbezogene Threat Intelligence Service AutoFocus™ bietet die notwendigen Informationen, Analysen und den Kontext, um zu erkennen, welche Angriffe eine sofortige Reaktion erfordern. Mit trennscharfen Bedrohungsindikatoren ermöglicht er die vorbeugende Verhinderung künftiger Angriffe.

Über uns

Prisma Cloud

Prisma® Cloud von Palo Alto Networks ist eine umfassende cloudnative Sicherheitsplattform, die mit branchenführenden Sicherheits- und Compliancefunktionen Anwendungen, Daten und cloudnative Technologien in Multi- und Hybrid-Cloud-Umgebungen während des gesamten Entwicklungslebenszyklus schützt.

Unit 42

Unit 42 ist das globale Threat Intelligence Team von Palo Alto Networks. Unsere Analysten sind spezialisiert auf die Suche nach und die Erfassung von Cyberbedrohungstaktiken und -techniken sowie das Reverse Engineering von Malware, um nach Möglichkeit ihren technischen Kontext zu erkennen. Unit 42 verbindet Threat Intelligence mit den Produkten von Palo Alto Networks, damit Kunden über die gesamte Sicherheitssuite hinweg geschützt sind.

Autoren

Jay Chen, Senior Threat Researcher, Public Cloud Security, Palo Alto Networks

Nathaniel „Q“ Quist, Senior Threat Researcher, Public Cloud Security, Palo Alto Networks

Matthew Chiodi, Vice President und Chief Security Officer, Public Cloud, Palo Alto Networks

UNIT 42
BY PALO ALTO NETWORKS

Oval Tower, De Entrée 99–197
1101 HE Amsterdam, Niederlande
Telefon: +31 20 888 1883
Vertrieb: +800 723 9771
Support: +31 20 808 4600
www.paloaltonetworks.de

© 2021 Palo Alto Networks, Inc. Palo Alto Networks ist eine eingetragene Marke von Palo Alto Networks. Eine Liste unserer Marken ist unter https://www.paloaltonetworks.com/company/trademarks.html verfügbar. Alle anderen hier erwähnten Marken können Markenzeichen der jeweiligen Unternehmen sein. Palo Alto Networks übernimmt keine Haftung für Ungenauigkeiten in diesem Dokument und lehnt jede Verpflichtung ab, die darin enthaltenen Informationen zu aktualisieren. Palo Alto Networks behält sich das Recht vor, dieses Dokument ohne vorherige Benachrichtigung zu ändern, zu bearbeiten, zu übertragen oder auf andere Weise zu überarbeiten.
unit42_cloud-threat-report-1h-2021_040121-de