netskope

DIE DUNKLE SEITE DER CLOUD

CLOUD-BASIERTE BEDROHUNGEN SIND AUF DEM VORMARSCH & SENSIBLE DATEN BEWEGEN SICH ZWISCHEN DEN CLOUD-APPS

PRÄSENTIERT VON:

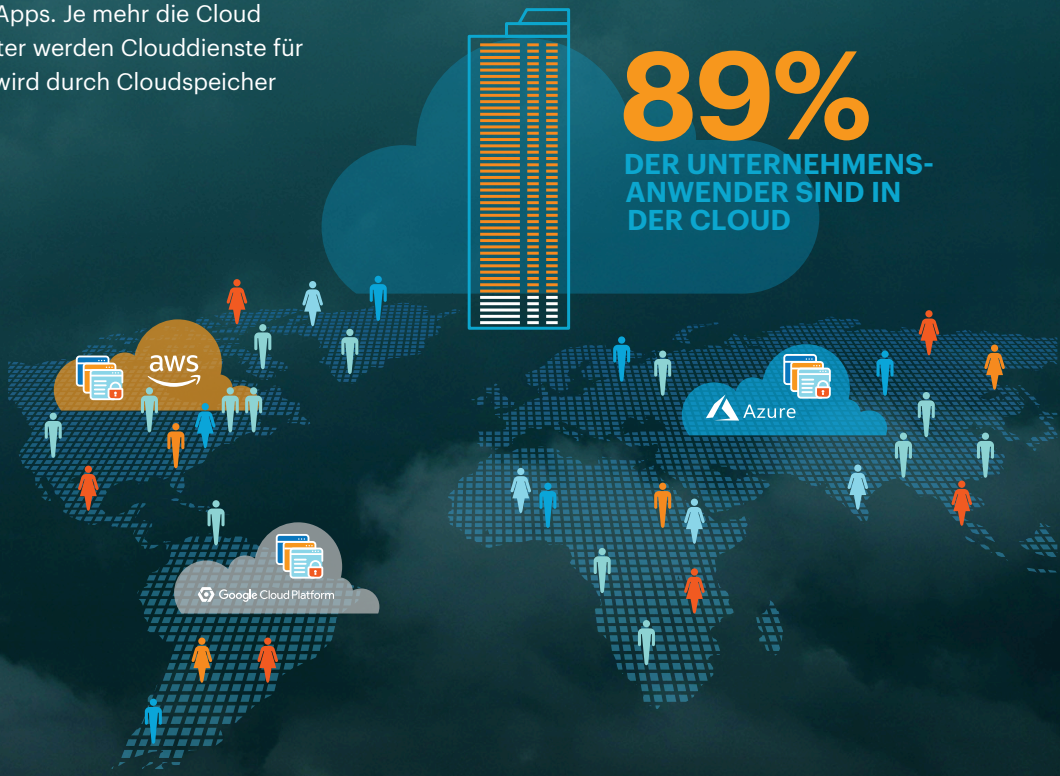
netskope
THREAT LABS

KURZFASSUNG

Durch den digitalen Wandel nutzen Unternehmen verstärkt Clouddienste und -Apps. Je mehr die Cloud an Bedeutung gewinnt, desto deutlicher werden ihre Schattenseiten. Immer öfter werden Clouddienste für unterschiedliche Phasen der Cyber Kill Chain genutzt und die Datensicherheit wird durch Cloudspeicher und -dienste immer stärker gefährdet.

Dieser Bericht liefert Erkenntnisse über die Entstehung cloudbasierter Bedrohungen und die Übertragung sensibler Daten in die Cloud und aus der Cloud – und wie dies die Sicherheitslage von Unternehmen verkompliziert. Dazu kommt nun auch noch die Umkehr des Netzwerk-Traffics durch die ständig zunehmende Zahl von Mobil- und Remotenutzern, die immer öfter auf öffentliche und private Anwendungen in der Cloud zugreifen. So steigt das Risiko für Unternehmen und neue Sicherheitsarchitekturen und -ansätze werden notwendig. Außerdem sind veraltete Sicherheitssysteme nicht in der Lage, den Traffic von gemanagten und nicht gemanagten Clouddiensten und -Apps und ältere Anwendungen nicht leistungsstark genug, um TLS-verschlüsselten Cloud- und Web-Traffic zu entschlüsseln. Das Ergebnis: Verwaltete Clouddienste werden auf die weiße Liste gesetzt, um wichtige Abwehrmaßnahmen zu umgehen, wodurch wiederum der Weg für cloudbasierte Bedrohungen geebnet wird.

Dieser Bericht basiert auf anonymisierten Daten, die im Zeitraum vom 1. August bis 31. Dezember 2019 von Millionen von Nutzern der Netskope Security Platform erhoben wurden.



ÜBERBLICK

- 89 % der Enterprise-Nutzer arbeiten mit gemanagten und ungemanagten Clouddiensten und -Apps.
- 44 % der Angreifer nutzen die Schwächen von Clouddiensten in den unterschiedlichen Phasen der Cyber Kill Chain aus.
- 20 % der Nutzer verschieben Daten zwischen verwalteten und nicht verwalteten Clouddiensten sowie zwischen beruflichen und privaten Instanzen.
- > 50 % der Verstöße gegen Datenschutzrichtlinien entstehen in Cloudspeicher-, Kollaborations- und Webmail-Apps.
- 33 % der Enterprise-Nutzer arbeiten remote.

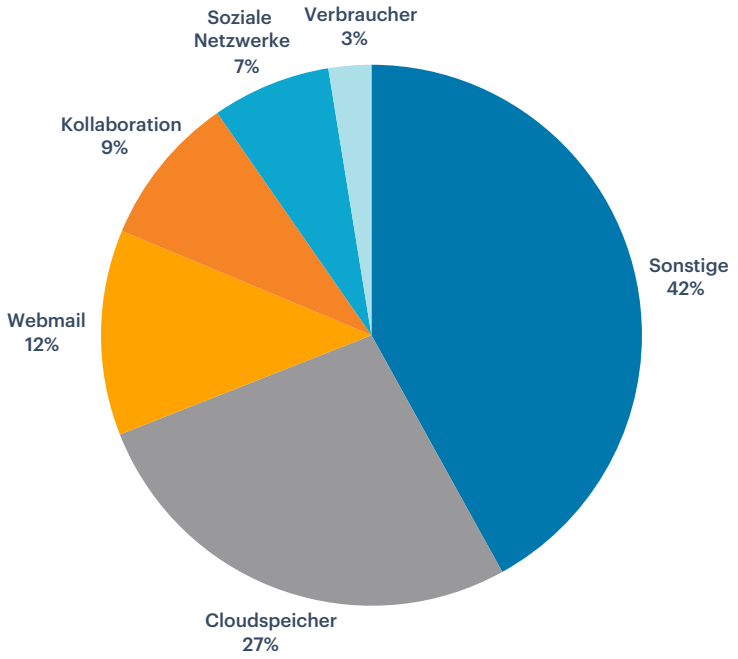
CLOUDBASIERTE BEDROHUNGEN NEHMEN ZU

Die Cyberkriminalität ist weiterhin finanzstark und gut organisiert. Ihr Ziel ist es, ihre Erfolgsraten zu steigern und zu verhindern, dass Angriffe entdeckt werden. Eine beliebte Strategie besteht darin, sich die Hot-Spots des Internets zunutze zu machen, an denen die wertvollsten Nutzer zu finden sind. Dieser Trend spiegelt sich in der Liste der am stärksten bedrohten Websitekategorien wider – und lässt auf Empfehlungen für die Nutzung von Clouddiensten und -Apps schließen.

1. Contentserver
2. Onlineanzeigen
3. Private Websites und Blogs

Die Top-Kategorien sind keine Hochrisikokategorien wie Bulletproof-Hosting-Anbieter und neu registrierte Domains. Stattdessen verstecken sich Angreifer im Mainstream und verbreiten Bedrohungen über beliebte Websitekategorien. Ein Beispiel dafür ist eine breit angelegte Adware-Kampagne, die sich über infizierte Chrome-Erweiterungen verbreitet hat.

Im folgenden Diagramm ist aufgeschlüsselt, welche Kategorien von Cloud-Apps Angreifer missbrauchen: Die meisten Cloudbedrohungen fallen unter die Top 5-Kategorien der Clouddienste und -Apps: Cloudspeicher, Webmail, Kollaboration, Soziale Netzwerke und Verbraucher. Die verbleibenden 42 % verteilen sich auf die übrigen 24 Kategorien.



Durch den digitalen Wandel hat sich die Nutzung von Cloudanwendungen im Enterprise-Bereich stark erhöht: 89 % der Nutzer sind aktiv und machen Cloud-Apps zum neuen „Hot-Spot“. Angreifer verlagern ihre Aktivitäten ebenfalls in die Cloud, um nicht aufzufallen. Dadurch steigern sie ihre Erfolgsraten und bleiben unentdeckt. Angriffe erfolgen über Clouddienste und -Apps. Dabei setzen die Angreifer weiterhin bewährte Taktiken ein, beispielsweise Scams, Phishing, Malware-Zustellung, Command-and-Control, Formjacking, Chatbots und Datenexfiltration. Die beiden beliebtesten Bedrohungstechniken in der Cloud sind Phishing und Malware-Zustellung.

Während der zweiten Jahreshälfte 2019 identifizierten die Netskope Threat Labs 44 % aller böswilligen Bedrohungen als cloudbasiert. Insgesamt hatten die Angreifer es auf die beliebtesten Clouddienste und -Apps abgesehen und dabei das stillschweigende Vertrauen der Nutzer und Admins ausgenutzt. Einige dieser Apps standen sogar auf der weißen Liste, sodass wichtige Abwehrmechanismen umgangen werden konnten und Angreifern Tür und Tor geöffnet wurden. Die folgende Liste verdeutlicht diesen Trend: Die fünf Top-Apps, bei denen Netskope Bedrohungen erkennt, gehören auch zu den beliebtesten Clouddiensten und -Apps im Enterprise-Bereich:

1. Microsoft Office 365 OneDrive for Business
2. Box
3. Google Drive
4. Microsoft Azure
5. GitHub

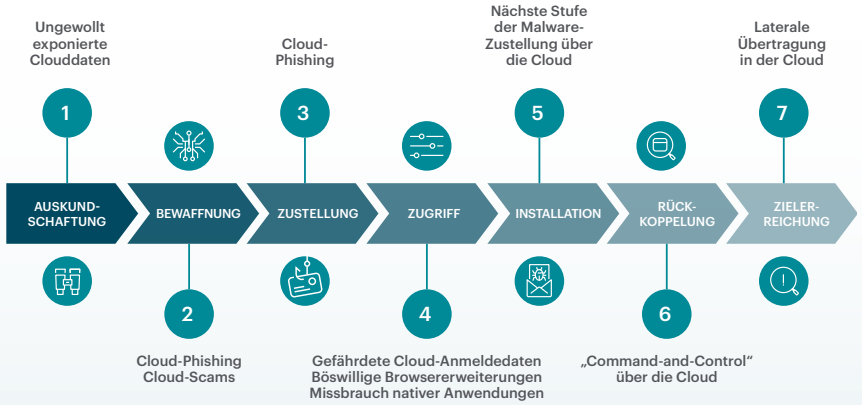
Cloudbedrohungen und die entsprechenden Abwehrmaßnahmen lassen sich mithilfe der Cloud Kill Chain und der Mitre Cloud ATT&CK Matrix veranschaulichen. Insgesamt hat Netskope Threat Labs Cloudbedrohungen in 1.609 unterschiedlichen Clouddiensten und -Apps erkannt. Das zeigt, wie verbreitet Cyberkriminalität mittlerweile ist.

Sicherheitsmaßnahmen, die sich lediglich auf eine Handvoll verwalteter Clouddienste und -Apps beschränken, werden das Problem nicht lösen können. Nur wenn wir den Schutz vor Bedrohungen und die Datensicherheit Tausender verwalteter und nicht verwalteter Clouddienste und -Apps entschlüsseln, können wir umfassende Antworten auf die Herausforderungen finden, vor die uns Angreifer im Zuge des Wechsels zur Cloud Kill Chain stellen.

CLOUD ATT&CK MATRIX

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation	Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Exploit Public-Facing Application	Create Account		Redundant Access	Brute Force	Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Spearphishing Link	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Web Session Cookie	Data from Local System		
Trusted Relationship	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning		Data Staged		
Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access Token	Network Share Discovery		Email Collection		
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie	Permission Groups Discovery				
					Remote System Discovery				
					System Information Discovery				
					System Network Connections Discovery				

CLOUD KILL CHAIN



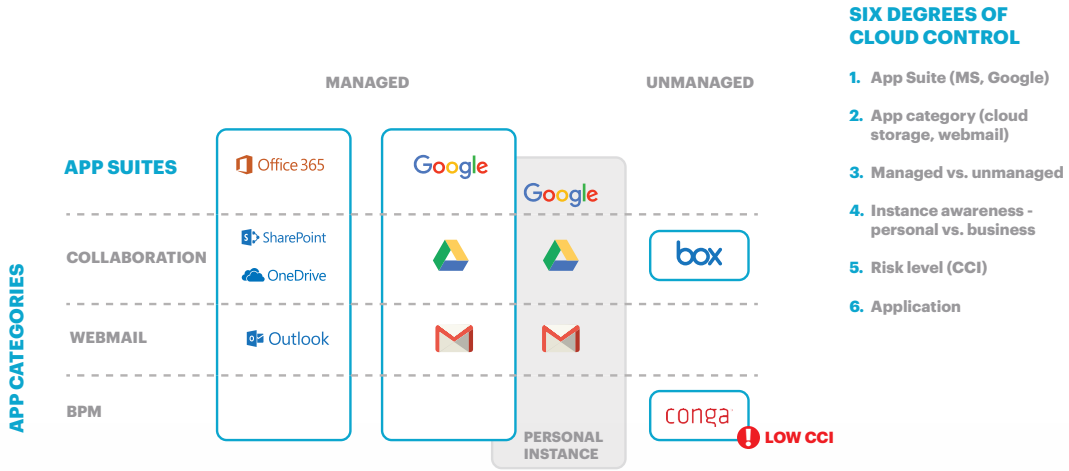
DIE SENSIBLEN DATEN SIND IM UMLAUF

Organisationen, die die Cloud benutzen, genehmigen nur bestimmte Kontoinstanzen von Cloudanwendungen, um dort ihre sensiblen Daten zu speichern. Im Prinzip ist das eine gute Strategie. Studien von Netskope zeigen jedoch, dass Nutzer – entgegen bestehender Organisationsrichtlinien – sensible Daten über mehrere Dimensionen hinweg in eine Vielzahl von Clouddiensten und -Apps übertragen, darunter auch persönliche Instanzen und nicht verwaltete Apps. Die Mehrzahl der Verstöße gegen Datenschutzrichtlinien entstehen durch Cloudspeicher-, Kollaborations- und Webmail-Apps. Die 10 häufigsten Clouddienste und -Apps in diesen Kategorien sind:

1. Microsoft Office 365 Outlook.com
2. Microsoft Office 365 OneDrive for Business
3. Microsoft Office 365 Sharepoint Sites
4. Box
5. Google Gmail
6. Google Drive
7. Salesforce.com
8. Egnyte
9. Microsoft OneDrive
10. Amazon S3

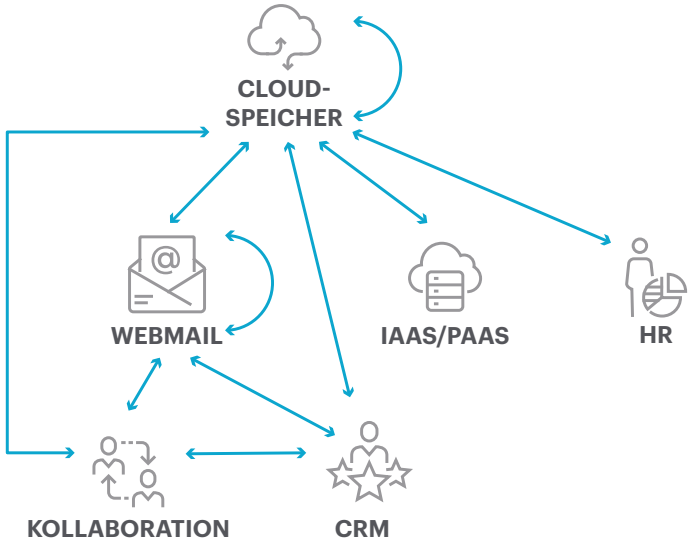
Die Arten von Daten, um die es bei diesen Verstößen gegen die Datenrichtlinien geht, fallen hauptsächlich in die Bereiche Datenschutz, Gesundheitswesen und Finanzen:

- Personenbezogene Daten
- Datenschutz-Grundverordnung (DSGVO)
- Geschützte medizinische Daten
- Zahlungskartendaten
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Gramm-Leach-Bliley Act (GLBA)
- Quellcode
- Passwörter, Anmeldedaten und Schlüssel



Außerdem fällt auf, dass es immer häufiger zur Übertragung sensibler Daten zwischen Clouddiensten und -Apps kommt, unter anderem zwischen verwalteten und nicht verwalteten Clouddiensten und -Apps sowie zwischen beruflichen und privaten Instanzen. Mindestens 20 % der Enterprise-Nutzer übertragen Daten lateral zwischen Cloudanwendungen. Entscheidend ist hier: Die Daten überschreiten viele Grenzen. Sie werden zwischen App-Suiten übertragen, zwischen verwalteten und nicht verwalteten Apps, zwischen App-Kategorien und zwischen Apps verschiedener Risikostufen (Netskope Cloud Confidence Levels). Darüber hinaus handelt es sich bei 37 % der Daten, die Nutzer an andere Cloud-Apps übertragen, um sensible Daten. Insgesamt hat Netskope laterale Datenübertragungen zwischen 2.481 unterschiedlichen Clouddiensten und -Apps festgestellt. Dies zeigt, in welchem Ausmaß sensible Daten in unterschiedlichsten Cloudanwendungen verteilt werden.

Bestimmte Arten von App-übergreifenden Datenübertragungen kommen häufiger vor als andere. In der folgenden Liste sind die Kombinationen von App-Kategorien mit den meisten App-übergreifenden Übertragungen aufgeführt. Am häufigsten finden Datenübertragungen zwischen unterschiedlichen Cloudspeicher-Apps oder zwischen Cloudspeicher-Apps und Apps anderer Kategorien statt. Übertragungen zwischen verschiedenen Webmail-Apps haben es ebenfalls unter die Top 10 geschafft. Dies deutet darauf hin, dass Nutzer mehrere Webmail-Apps nutzen, um Dateien unternehmensintern und außerhalb des Unternehmens zu teilen: Cloud-Apps und Dienste sind außerdem häufig eine Quelle für Datenlecks, weil es mit ihnen so einfach ist, Daten zu teilen.



1. Cloudspeicher ⟷ Cloudspeicher
2. Cloudspeicher ⟷ Kollaboration
3. Cloudspeicher ⟷ Webmail
4. Cloudspeicher ⟷ CRM
5. Webmail ⟷ CRM
6. Webmail ⟷ Kollaboration
7. Kollaboration ⟷ CRM
8. Cloudspeicher ⟷ IaaS/PaaS
9. Cloudspeicher ⟷ HR
10. Webmail ⟷ Webmail

Die weit verbreitete Übertragung von Daten in die Cloud erfordert bessere Überwachung, Kontrolle und Governance. Veraltete Sicherheitsmaßnahmen sind nicht in der Lage, Clouddienste und -Apps zu dekodieren. Dadurch fehlt es an Transparenz und Kontrolle über diese Datenübertragungen in der Cloud und Unternehmen sind potenziellen Datenlecks und -diebstählen ausgesetzt. Darüber hinaus machen ungeschützte Daten in Cloudspeicherlösungen immer wieder Schlagzeilen. Dabei können fortlaufende Sicherheitsbewertungen mit Regeln und automatisierter Nachbesserung das Risiko effektiv mindern.

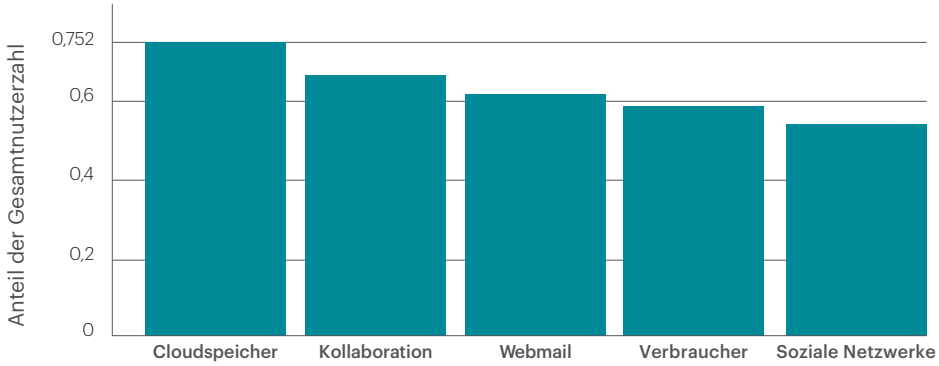
DAS NETZWERK DREHT SICH VON INNEN NACH AUSSEN: NUTZER, DATEN UND APPS SIND AUSSERHALB

In Organisationen, die die Cloud benutzen, sind drei Trends erkennbar, die eine Umkehr des traditionellen Netzwerks darstellen:

- Zunehmende Nutzung öffentlicher Clouddienste und -Apps
- Zunehmende Remote-Arbeit, zumindest stundenweise auch für reguläre Büroangestellte
- Migration von privaten Apps und Daten in die Cloud

Im Durchschnitt verwendet eine einzige Organisation 285 verschiedene Clouddienste und -Apps in den wichtigsten drei Kategorien: Cloudspeicher, Kollaboration und Webmail. Insgesamt nutzen durchschnittliche Unternehmen 2.415 verschiedene Clouddienste und -Apps. Hier die Top 10 Apps:

1. Google Drive
2. YouTube
3. Microsoft Office 365 OneDrive for Business
4. Facebook
5. Google Gmail
6. Microsoft Office 365 Sharepoint Sites
7. Microsoft Office 365 Outlook.com
8. Twitter
9. Amazon S3
10. LinkedIn



Zunehmende Telearbeit

Im Durchschnitt arbeiten jeden Tag 33 % der Nutzer in einem Unternehmen von einem Remote-Standort aus. Bei den Top 10 % der Organisationen im Bereich Telearbeit sind 80 % der Mitarbeiter außerhalb des Büros tätig. Außerdem sind die Nutzer mobil: Im Durchschnitt arbeiten Nutzer von 8 verschiedenen Standorten aus. Die Top 10 % der Telearbeiter arbeiten von mindestens 18 Standorten aus. Dieser Trend führt zu immer höheren Ansprüchen an ältere VPNs und stellt die Verfügbarkeit von Sicherheitsmaßnahmen zum Schutz von Telearbeitern in Frage. Die Evolution von Zero-Trust-Netzwerkzugriffen und hochverfügbaren nativen Sicherheitsmaßnahmen für die Cloud sorgen für eine sichere, risikoärmere Alternative.

Migration privater Apps in die Cloud

Organisationen verlagern außerdem intern entwickelte Apps und Daten zu öffentlichen Cloudanbietern wie AWS, Azure und GCP. Studien von Netskope zeigen, dass Organisationen, die AWS, Azure oder GCP für private Apps verwenden, im Durchschnitt über 300 private Compute Instances in 3 Regionen bereitgestellt haben. Die Top 10 % stellen private Instanzen bei mehreren Cloudanbietern in mindestens 7 Regionen bereit. Wenn Sie Ihre eigenen Apps in der privaten oder öffentlichen Cloud ausführen möchten, müssen Sie auch sicherstellen, dass alle regulatorischen Standards eingehalten werden und keine neuen Schwachstellen entstehen.

Es findet gerade eine Netzwerktransformation statt: Nutzer sind immer mobiler und zunehmend mehr Apps und Dienste werden in die Cloud verlagert. Damit befindet sich auch die Enterprise-Sicherheit im Wandel – Daten müssen geschützt werden, wo immer sie sich auch befinden, und das Zero-Trust-Netzwerkmodell muss an das Cloudzeitalter angepasst werden.

CLOUD-SICHERHEIT

BEST PRACTICES UND EMPFEHLUNGEN

1 Überwachen Sie sämtlichen Web- und Cloudtraffic auf böswillige Bedrohungen wie Cloud-Phishing und Malware. Prüfen Sie Inhalte, Instanzen und Aktivitäten auf Bedrohungen – egal, aus welcher Quelle.

2 Implementieren Sie Cloud-DLP-Fähigkeiten, um Ihre Daten zu schützen, die in die Cloud und lateral zwischen Clouddiensten oder -Apps übertragen werden. Etablieren Sie DLP-Richtlinien und -Regeln mit granularen Kontrollen auf Aktivitätsebene, Erkennung von Anwendungsinstanzen und adaptiven Verhaltensanalysen. Auch bekannte behördliche DLP-Compliance-Richtlinien wie die DSGVO sollten eingehalten werden.

3 Geben Sie Ihren Mitarbeitern die Möglichkeit über eine flexible, skalierbare Lösung mit privatem Zugang von überall aus zu arbeiten. Implementieren Sie cloudnative Inline- und API-basierte Sicherheitsmaßnahmen, um sämtliche Daten und Geräte Ihrer Mitarbeiter zu schützen.

WEITERE INFORMATIONEN

Weitere Informationen zu cloudbasierten Bedrohungen und den neuesten Erkenntnissen der Netskope Threat Labs finden Sie unter: https://www.netskope.com/resources/netskope-threat-research-labs.

Weitere Informationen zu Tools, mit denen sich cloudbasierte Bedrohungen mindern lassen, finden Sie unter:

WWW.NETSKOPE.COM/PRODUCTS/NEXT-GEN-SWG

2020 © Netskope, Inc. All rights reserved. Netskope is a registered trademark and Netskope Active, Netskope Discovery, Cloud Confidence Index, and SkopeSights are a trademarks of Netskope, Inc. All other trademarks are trademarks of their respective holders. 02/20 RS-371-1