
TREND MICRO
research
MISCONFIGURED
THE FUTURE IS
Cloud- und DevOps-Migrationen bringen den Beteiligten viele Vorteile, sind aber auch mit Risiken verbunden, die die Notwendigkeit einer durchgängigen Sicherheit während der gesamten Bereitstellungs-Pipeline hervorheben.

Die Zukunft erscheint fehlkonfiguriert

Die Zukunft der Unternehmensinfrastrukturen liegt in der Cloud, deren volles Potenzial mithilfe einer DevOps-Kultur ausgeschöpft wird. Die Cloud kommt mit einer Fülle neuer Möglichkeiten und bietet Unternehmen größere Flexibilität, Skalierbarkeit und Kosteneinsparungen, die letztendlich einen Wettbewerbsvorteil darstellen. Doch Cloud- und DevOps-Migrationen bergen auch einige ernstzunehmende Risiken, die, wenn sie nicht richtig gehandhabt werden, das Unternehmen angreifbar machen. Trend Micro Research hat Vorhersagen für das Jahr 2020 erstellt, die sich auf die Ansichten und Erkenntnisse unserer Experten zu aktuellen und neuartigen Bedrohungen und Technologien stützen. Und es ist nicht weiter verwunderlich, dass Fehlkonfigurationen der Cloud dabei im Vordergrund stehen.

Schwachstellen in Container-Komponenten sind Top-Sicherheitsanliegen für DevOps-Teams

Der Bereich der Container[1] ist äußerst schnelllebig: Releases folgen schnell aufeinander, Architekturen werden kontinuierlich integriert und Softwareversionen regelmäßig aktualisiert. Herkömmliche Sicherheitsverfahren können hier nicht mithalten.

Diese Voraussetzungen zeigen noch einmal mehr, wie wichtig die DevSecOps-Prinzipien für DevOps-Teams sind, weil Container Konventionen auf den Kopf stellen und mehr Rollen übernehmen, die für Organisationen entscheidend sind. Schnelle Entwicklungszyklen lassen unter Umständen wenig Raum für Sicherheits- und Schwachstellentests, und eine Anwendung kann es erforderlich machen, Hunderte von Containern zu sichern, die auf mehrere virtuelle Maschinen in verschiedenen Cloud-Service-Plattformen verteilt sind.

Unternehmen werden alle Hände voll zu tun haben, um die unterschiedlichen Komponenten der Containerarchitektur, einschließlich der Sicherheitslücken in Runtimes (z.B. Docker®, CRI-O, Containerd und runC[2]) über Orchestratoren (z.B. Kubernetes®) bis hin zu Entwicklungsumgebungen (z.B. Jenkins®) im Auge behalten. Angreifer finden immer Möglichkeiten, jeden Schwachpunkt dafür zu missbrauchen, die DevOps Pipeline zu kompromittieren.

Schwachstellen in weit verbreiteten Container-Images können Schaden in der Unternehmens-Pipeline bewirken, wenn sie anschließend heruntergeladen werden. Das Patchen von Containern wird besonders schwierig, wenn Unternehmen sich beim Fixen von Images auf Drittanbieter verlassen und darauf vertrauen, dass diese sicher sind. Schwachstellen in containerbasierten Anwendungen wirken sich nicht nur auf den Container-Code oder die Engine aus, sondern auch auf die vielen anderen Elemente des Stacks, in die böswillige Akteure eindringen können, um Zugriff und Kontrolle zu erlangen.

Serverlose Plattformen werden durch Fehlkonfigurationen und sicherheits-anfälligem Code Angriffsflächen bieten

Immer mehr Unternehmen setzen auf serverlose Plattformen, um Cloud-Anwendungen zu integrieren und Kosten zu sparen. Gartner geht davon aus, dass mehr als 20% der Unternehmen weltweit bis 2020 serverlose Technologien im Einsatz haben werden.[3] Serverlose Plattformen bieten „Function as a Service“ und ermöglichen Entwicklern die Ausführung von Code, ohne dass das Unternehmen für ganze Server oder Container bezahlen muss.[4] Doch der Einsatz serverloser Technologie bedeutet keine Immunität gegen Sicherheitsprobleme.

Wir erwarten, dass veraltete Bibliotheken, Fehlkonfigurationen sowie bekannte und unbekannte Schwachstellen die Eintrittspunkte von Angreifern in serverlose Anwendungen sein werden. Angreifer können diese dazu nutzen, sensible Informationen zu sammeln oder tiefer ins Unternehmensnetzwerk einzudringen.[5]

Serverlose Plattformen schließen Container, serverlose Funktionen und weitere Abhängigkeiten mit ein. Damit erhöht sich die Komplexität bei der Suche nach dem Ursprung einer Bedrohung noch mehr. Da serverloses Computing Funktionen -- insbesondere solche, die Open Source sind -- als zustandslos erscheinen lässt, werden die Überwachung von Berechtigungen und die Speicherung sensibler Daten 2020 ebenfalls zu den wichtigsten Anliegen gehören. Neben höherer Netzwerktransparenz sind die Verbesserung von Prozessen und die Dokumentation von Arbeitsabläufen für den Betrieb von serverlosen Anwendungen unerlässlich.

Wie bei Container-basierten Anwendungen sollte DevSecOps auch bei serverlosen Implementierungen an vorderster Front stehen. Serverlose Umgebungen werden zudem auch von der andauernden Integration und der Benutzerfreundlichkeit profitieren, die DevSecOps anstrebt.[6] Sicherheitswerkzeuge, die auf serverlose Infrastrukturen zugeschnitten sind, einschließlich auf Abhängigkeiten von Open-Source-Anwendungen und Schwachstellen, werden bei der Einführung und dem Einsatz bestimmter serverloser Funktionen wichtig sein.

Fehlkonfigurationen von Nutzern und unsichere Beteiligung Dritter erhöhen die Risiken für Cloud-Plattformen

Trotz regelmäßiger Systemaktualisierungen und geeigneter Maßnahmen kann ein Unternehmen trotzdem noch in Gefahr sein, wenn es falsch konfigurierte Anwendungen und Authentifizierungsprobleme beim Einsatz gibt. Grundlegende Sicherheitsmechanismen, die nicht ordnungsgemäß implementiert werden, stellen eine große Sicherheitsbedrohung für die Unternehmensdaten dar.

Wir rechnen mit einer Zunahme von Vorfällen durch kompromittierte Netzwerke aufgrund der Schwachstellen in Cloud-Diensten. Fehlkonfigurationen in Cloud-Speichern, die zu Datenlecks führen, werden auch im Jahr 2020 noch ein häufiges Sicherheitsproblem darstellen. Unzureichende Zugriffsbeschränkungen, schlecht verwaltete Berechtigungskontrollen, Nachlässigkeit bei der Protokollierung von Aktivitäten und öffentlich zugängliche Assets sind nur einige der Fehler, die Unternehmen bei der Einrichtung ihrer Cloud-Netzwerke begehen werden. Fehler und Ausfälle im Zusammenhang mit Cloud-Diensten können eine beträchtliche Anzahl von Firmendaten exponieren und sogar zu Geldstrafen führen. Diese Risiken lassen sich eindämmen, wenn Unternehmen ihre generelle Sicherheitshaltung in der Cloud verbessern. Dies bedeutet, dass sie Infrastrukturen richtig konfigurieren und bereitstellen und dass sichergestellt ist, dass Best Practices und Industriestandards eingehalten werden.

Bei steigender Zahl von Cloud-Migrationen in Unternehmen und in der Fertigung (z.B. Produktionsanlagen)[7], kommen auch immer mehr Dritt-Service Provider ins Spiel. Dabei besteht jedoch auch das Risiko, dass diese Anbieter keine Erfahrung mit der Cloud haben und nicht darauf eingerichtet sind, die Infrastruktur zu schützen. Angreifer fühlen sich dazu ermutigt, DDoS-Angriffe gegen Dienstanbieter über Botnets durchzuführen, um Cloud-Dienste zu behindern oder gar zu unterbrechen.

Cloud-Plattformen werden Opfer von Code-Injection-Angriffen über Drittanbieter-Bibliotheken

2020 wird es mehr Angriffe auf Cloud-Plattformen über Code Injection geben, sei es direkt im Code oder über Bibliotheken Dritter. Das Einschleusen von Malware kann entweder beim Mithören der Dateien und Informationen eines Benutzers in der Cloud erfolgen oder durch die Übernahme der Kontrolle darüber. Häufige Formen solcher Angriffe in Webanwendungen von Cloud-Diensten sind Cross-Site-Scripting- und SQL-Injection-Angriffe. Bei Erfolg können Hacker heikle Daten aus der Ferne abrufen und Datenbankinhalte manipulieren. Auch können Angreifer mit Drittanbieter-Bibliotheken einen anderen Weg einschlagen, sodass sie, wenn sie von Benutzern heruntergeladen werden, injizierten bösartigen Code ausführen.[8]

Trend Micro geht davon aus, dass mehr Angreifer Daten in die Cloud folgen werden. Cloud-Einbrüche werden passieren, da der Einsatz von Software-, Infrastruktur- und Platform-as-a-Service-Cloud-Computing-Modellen weiterhin zunimmt. Je mehr Unternehmensdaten in der Cloud liegen, desto größer wird das Interesse böswilliger Akteure. Um Cloud-Kompromittierungen zu verhindern, bedarf es der gebührenden Sorgfalt der Entwickler, einer sorgfältigen Prüfung der Anbieter und der angebotenen Plattformen sowie einer Verbesserung des Sicherheitsmanagements in der Cloud.

Fazit

Vorbei sind die Zeiten von Netzwerken, die isoliert hinter einer Firmen-Firewall und einem begrenzten Stack von Unternehmensanwendungen arbeiten. Während sich die Welt verändert, um agiler und flexibler zu werden, gilt dies für die Cybersicherheit genauso. Cloud Computing benötigt eine größere Sichtbarkeit und Kontrolle über alle beweglichen Teile, um Schwachstellen und Fehlkonfigurationen, die sich in der Komplexität der Cloud verbergen, erkennen und beheben zu können. Anderenfalls hinterlassen DevOps und Cloud-Sicherheitsteams in Multi-Cloud-Umgebungen nicht beherrschbare Risiken, die zu erheblichen Einnahme-, Reputations- und Zeitverlusten führen können. Um dies zu vermeiden, muss die Sicherheit aus vielen Gesichtspunkten heraus betrachtet werden, um mit den Cyberkriminellen und neuen Akteuren sowie deren Taktikwechseln Schritt zu halten und ihnen zuvorzukommen. Das klingt zwar im ersten Moment wie eine unüberwindliche Hürde, doch mit den richtigen Werkzeugen, bewährten Verfahren und einer fundierten Entscheidungsfindung können Unternehmen Sicherheit mit der Schnelligkeit und Einfachheit erreichen, die erforderlich sind, um mit der Cloud Schritt zu halten.

1. Trend Micro. (n.d.). Trend Micro. "Container." Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/definition/container.
2. Trend Micro. (28 February 2019). Trend Micro Security News. "CVE-2019-5736: RunC Container Escape Vulnerability Provides Root Access to the Target Machine." Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/cve-2019-5736-runc-container-escape-vulnerability-provides-root-access-to-the-target-machine.
3. Gartner, Inc. (4 December 2018). Gartner. "Gartner Identifies the Top 10 Trends Impacting Infrastructure and Operations for 2019." Last accessed on 24 October 2019 at https://www.gartner.com/en/newsroom/press-releases/2018-12-04-gartner-identifies-the-top-10-trends-impacting-infras.
4. Scott Fulton III. (9 April 2019). ZDNet. "What serverless computing really means, and everything else you need to know." Last accessed on 24 October 2019 at https://www.zdnet.com/article/what-serverless-computing-really-means-and-everything-else-you-need-to-know/.
5. Guy Podjarny. (15 May 2018). The Register. "Hey cool, you went serverless. Now you just have to worry about all those stale functions." Last accessed on 10 October 2019 at https://www.theregister.co.uk/2018/05/15/stale_serverless_functions/.
6. Trend Micro. (13 April 2018). Trend Micro Security News. "Serverless Applications: What They Mean in DevOps." Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/serverless-applications-what-they-mean-in-devops.
7. Willem Sundblad. (18 July 2019). Forbes. "Smart Manufacturing: Creating a Hybrid Cloud-Edge Strategy." Last accessed on 10 October 2019 at https://www.forbes.com/sites/willemsundbladeurope/2019/07/18/smart-manufacturing-creating-a-hybrid-cloud-edge-strategy/#77fc5816af5a.
8. Trend Micro. (29 November 2018). Trend Micro Security News. "Hacker Infects Node.js Package to Steal from Bitcoin Wallets." Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hacker-infects-node-js-package-to-stealfrom-bitcoin-wallets.

For Raimund Genes (1963-2017)

TREND MICRO™ | research

Trend Micro Security Predictions for 2020

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next wave of threats and deliver thought-provoking research that can shape strategic industry direction.

www.trendmicro.com