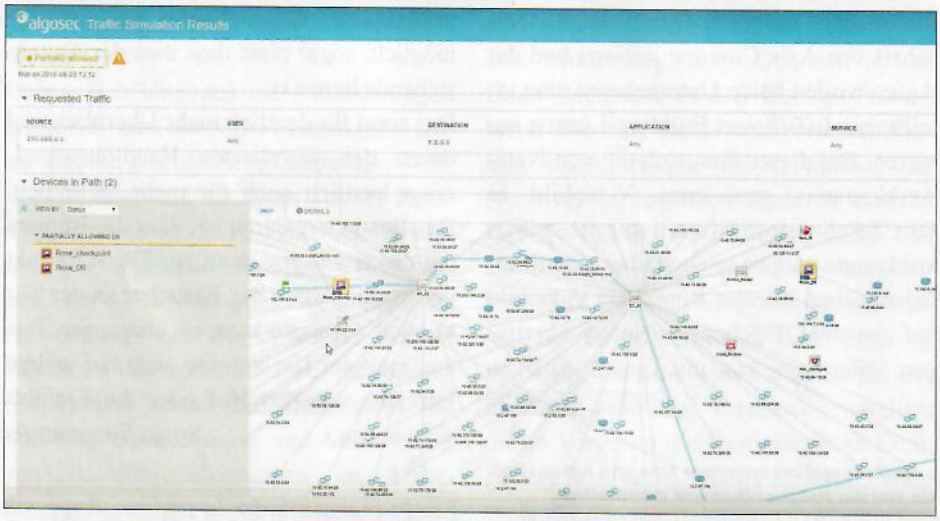
DevOps-freundliche Netzwerksicherheit

Agile Entwicklung trifft Security

DevOps dreht sich um Agilität mittels schneller, kurzer Lieferzyklen sowie um die Automation von Softwareentwicklung und Applikationen. Virtualisierung, Cloud und SDN (Software-Defined Networking) ermöglichen das Hochfahren neuer Server, die Bereitstellung von Speicherplatz in einer öffentlichen oder privaten Cloud und selbst das Starten ganzer Umgebungen in Minuten- oder gar Sekundenschnelle. Erfordert eine neue Applikation, ein neuer Dienst oder eine neue Umgebung jedoch eine Änderung der Netzwerkanbindung oder der Firewall-Regeln, kann dies die Bereitstellung auf Schneckentempo verlangsamen.

Im typischen DevOps-Szenario erzeugen Entwickler eine CI/CD-Pipeline (Continuous Integration/Continuous Delivery), die Development, Test und automatische Bereitstellung der neuen Anwendung umfasst. Dem gegenüber ist die Provisionierung neuer Netzwerkverbindungen in der Regel ein mühsamer Prozess: Der Anwendungsentwickler muss eine Änderungsanforderung (Change Request) manuell öffnen und dann auf die Genehmigung und Implementierung der neuen Verbindung warten, bevor er mit dem DevOps-Ablauf fortfahren kann. Hierzu muss der Entwickler in den Änderungsanforderungen normalerweise Informationen zu Firewalls, Zonen, Subnetzen sowie andere Daten über die zugrunde liegende Netzwerkinfrastruktur bereitstellen – Informationen, die ihm nicht immer bekannt oder bewusst sind. Die Abteilung wiederum, die für die Implementierung der Änderungen zuständig ist, versteht die Anforderungen und deren Kontext häufig nicht. Dies kann zu einem Hin und Her in der Kommunikation zwischen Entwicklern und dem Netzwerk-Sicherheitsteam führen. Dies macht den gesamten Prozess für beide Gruppen extrem langwierig, fehleranfällig, ineffizient und frustrierend.



Die Traffic-Simulation einer NSPM-Lösung erleichtert DevOps-Prozesse. Bild: AlgoSec

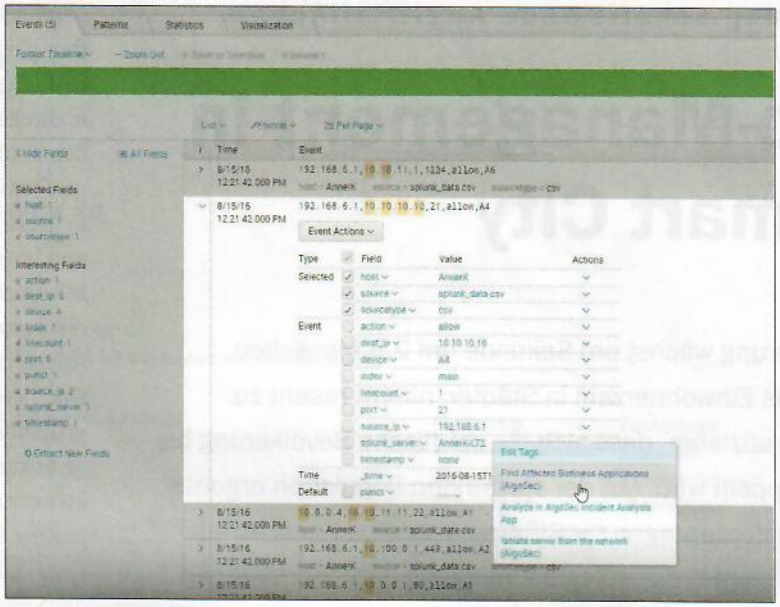
Die Herausforderung besteht darin, die erforderlichen Kontrollen und Gegenkontrollen vorzunehmen, um zu garantieren, dass DevOps-Prozesse nicht plötzlich Sicherheitsprobleme hervorrufen. Gleichzeitig muss gewährleistet sein, dass die Sicherheit nicht das Alltagsgeschäft ausbremst und die Agilität des Unternehmens einschränkt.

Connectivity as Code

Die Antwort auf diese Herausforderung lautet „Connectivity as Code". Diese Methode unterstützt nicht nur die Automatisierung und Flexibilität der Bereitstellung, sondern schließt auch kontinuierlich die Lücke zwischen Anwendungsentwicklern und der Netzwerksicherheit – selbst wenn die Anwendung bereits im produktiven Einsatz ist. Möglich wird dies durch eine Abstraktionsebene, die beiden Welten zur Verfügung steht. Anwendungsentwickler haben dadurch mehr Kontrolle über ihre Anwendungen, das Netzwerk-Sicherheitsteam kann die Auswirkungen der täglichen Aufgaben auf das Geschäft nachvollziehen und für Kontinuität sorgen.

Zur Umsetzung beschreibt der Anwendungsentwickler zunächst die Connectivity-Anforderungen der Applikation in einer einfachen, maschinenlesbaren Textdatei. Er listet alle logischen Abläufe im Zuge dieser Anforderungen auf, auch für die verschiedenen Anwendungsumgebungen (Test, Entwicklung, Produktion). Die Abläufe sind dann als Liste abstrakter Nachrichtenflüsse dargestellt. Diese enthält in der Regel Informationen wie die Quelle (also wer die Verbindung initiiert), das Ziel (also wer die Verbindung akzeptiert) sowie den Dienst und weitere Angaben. Der Entwickler muss dabei weder wissen, wo die Server stehen, wie die zugrunde liegende Netzwerktopologie aussieht (ob sich zwischen ihnen eine Firewall oder Cloud-

Security-Mechanismen befinden), noch muss er die IP-Adressen oder Subnetze kennen. Unerheblich ist hier auch, ob bereits eine Verbindung vorhanden ist, da andere Anwendungen diesen Link bereits benötigten.



Das NSPM-Tool ermittelt die einem Netzwerk-Link zugeordneten Applikationen. Bild: AlgoSec

Verbindungen herstellen und verwalten

Sobald diese Liste vorliegt, erledigt der nächste Schritt im DevOps-Prozess, die „Connectivity-Phase", die Aufgaben automatisch ohne Eingriff der Anwendungsentwickler. Nun erfolgt die eigentliche Bereitstellung und Validierung der Connectivity. Zum Einsatz kommt hier eine Lösung zur Verwaltung von Netzwerk-Sicherheitsrichtlinien (Network-Security-Policy-Management, NSPM). Sie automatisiert im Rahmen des DevOps-Prozesses die Bereitstellung der Netzwerkverbindungen – wie alle anderen Konfigurations- oder Bereitstellungsschritte – in der DevOps-Pipeline. Die NSPM-Lösung liest die Datei erst und überprüft automatisch, ob die Anforderungen sich geändert haben. Liegen keine Änderungen vor, prüft die Lösung, ob die erforderliche Netzwerkverbindung weiterhin besteht und die Applikation ordnungsgemäß funktioniert. So kann der Entwickler sicherstellen, dass die erforderliche Verbindung vorhanden ist und bei einem Produktionsstart keine Fehler zu erwarten sind.

Haben sich hingegen die Anforderungen geändert, nutzt die NSPM-Lösung die Datei, um die erforderliche Connectivity bereitzustellen, und speichert sie als Referenz. So bleiben die Angaben zur Vernetzung der Applikation für spätere Änderungen der Netzwerkarchitektur und für Anwendungs- oder Server-Migrationen erhalten. Ist einer oder sind mehrere der erforderlichen Flows blockiert, stößt die Software einen Prozess zur Anforderung von Richtlinienänderungen an. Dabei überprüft ein NSPM, ob die neuen Flows den von der Organisation genehmigten Sicherheitsrichtlinien, den Best Practices und Branchenvorgaben entsprechen. Die Lösung erstellt und implementiert dann die erforderlichen Änderungen in Minutenschnelle automatisch, auch direkt auf den verschiedenen Sicherheitsgeräten im Netzwerk.

Ist ein Change Request nicht regelkonform, leitet die Software dies zur Genehmigung durch die IT-Abteilung weiter. Sobald dies erfolgt ist, implementiert sie die Änderung automatisch. Damit muss der Entwickler keine Änderungsanforderung mehr manuell erstellen. Er aktualisiert im Zuge jeder neuen Version seiner Anwendung diese Liste der Netzwerkanforderungen. Nach Abschluss der Connectivity-Phase kann der DevOps-Prozess dann sicher zum nächsten Schritt übergehen.

Die Einführung der „Connectivity as Code"-Methodik in den DevOps-Prozess bietet also eine Reihe von Vorteilen: Erstens vereinfacht sie die Verwaltung der Netzwerkverbindungen. Dadurch wird der DevOps-Prozess wesentlich schneller und agiler. Zugleich ermöglicht dies eine reibungslose Bereitstellung aller Anwendungen. Es treten keine Out-of-Band-Requests mehr auf, die eine separate manuelle Behandlung erfordern. Zweitens ermöglicht dieses Vorgehen die kontinuierliche Compliance und deren Überprüfbarkeit: Während des gesamten Vorgangs entsprechen die Unternehmen mit Sicherheit den relevanten Richtlinien. Gleichzeitig protokolliert die Software Änderungen zum Zweck der Überprüfung vollständig. Und drittens schließlich bietet der Ansatz die Grundlage für den ununterbrochenen Geschäftsbetrieb: Die Connectivity-Anforderungen sind klar dokumentiert und auf dem neuesten Stand. Dies sorgt selbst bei Änderungen an Netzwerk, Infrastruktur oder Architektur für eine nur minimale Unterbrechung des Geschäftsablaufs.

Fazit

Connectivity as Code schließt dauerhaft die Lücke zwischen Anwendungsentwicklern und Netzwerk-Sicherheitsteam: von der Planung und Entwicklung über die Bereitstellung und den produktiven Einsatz bis zur Außerbetriebnahme. Das Konzept stellt sicher, dass Entwickler und Security-Personal das bekommen, was sie brauchen: Entwickler müssen sich keine Sorgen machen, dass die Sicherheit sie ausbremst, während die Sicherheitsabteilungen wissen, dass Risiko- und Compliance-Prüfungen während der Bereitstellung der Anwendungen bedacht sind, einschließlich vollständig protokollierter Änderungen. Bedenken Unternehmen die Netzwerk-Connectivity beim DevOps-Prozess, können sie eine schnelle Bereitstellung gewährleisten, ohne Kompromisse bei Sicherheit oder Compliance eingehen zu müssen. Robert Blank/wg

Robert Blank ist DACH Lead Regional Sales Manager bei AlgoSec, www.algosec.com.