Pressemitteilung
Paris, 9. März 2017

DenyAll stellt Automatisierung der IT-Sicherheit in den Fokus der neuen Produktversionen

DenyAll, der europäische Marktführer von Sicherheitslösungen für Webapplikationen und Schwachstellenmanagement, hat seine Produktlinien überarbeitet. Die neuen Features orientieren sich an den Bedürfnissen von DevOps-Teams und vereinfachen das Testen und Automatisieren von Webapplikationen, Webservices und von Programmschnittstellen (APIs).

Unternehmen müssen die digitale Transformation nutzen, um sich vom Wettbewerb abzuheben und um mehr Agilität zu gewinnen. Softwareentwickler und Systemadministratoren müssen dazu die Administrationsprozesse schnell umsetzen und gleichzeitig für ein hohes Maß an IT-Sicherheit sorgen. Um die Sicherheit der Applikationen zu gewährleisten braucht es daher Werkzeuge, die automatisiert arbeiten. Nur dann können DevOps-Teams Applikationen entwickeln, die dem Secure-by-Design-Ansatz entsprechen, und auf Schwachstellen getestet und vor automatischen Angriffen geschützt werden.

Automatisierung und einfache Administration sind daher die Kernelemente für alle Innovationen, die DenyAll in den neuen Versionen und Cloud-Diensten implementiert hat. Diese neuen Entwicklungen sind:

- Web Application Firewall (WAF) Version 6.3, inklusive der zugehörigen Module, Web Services Firewall (WSF) und Web Access Manager (WAM)
- Vulnerability Manager 6.5 (Ende März auf dem Markt)
- Cloud Protector, die vollautomatische WAF-as-a-Service des Unternehmens.

Neue Automatisierungs-Features

Die folgenden Produkt-Features sorgen für eine kürzere Administrationszeit und eine optimale Sicherheit:

1. **Konfiguration klonen:** Administratoren können in der DenyAll WAF ohne vorkonfigurierte HA Tunnel klonen. Dadurch werden die Tunnelkonfigurationen automatisch synchronisiert, wenn ein zusätzlicher Load Balancer vor die WAF gesetzt wird. Die neue Orchestrierungs-API unterstützt die Automatisierung von ähnlichen wiederkehrenden Verwaltungsaufgaben.
2. **Applikationen lernen:** Die neu gestaltete Sitemap-Funktion der DenyAll WAF ist in der Lage, automatisch HTTP-/REST-Apps und APIs aus Traffic Logs der Entwickler bzw. aus der Vorproduktion und OpenAPI-/Swagger-Dateien zu lernen. Sie lernt automatisch Pfade, Methoden und Parameter und spart damit wertvolle Zeit ein.
3. **Fehlalarme verwalten:** Durch ein neues Token-Konzept in der DenyAll WAF werden Fehlalarme leichter erkannt und behandelt. Dieses Feature ermöglicht die Bearbeitung von Alarmen, die die zahlreichen komplementären Sicherheitsinstrumente der Plattform auslösen, mit nur einem Klick. Die Instrumente verwenden neben Techniken zur negativen, positiven und heuristischen Analyse auch solche für Grammatik- und Normalisierungsanalysen und zur Analyse von Nutzerverhalten.
4. **Schwachstellenüberprüfung und Virtuelles Patching:** Der Vulnerability Manager kann mithilfe des neuen automatischen Webcrawlers oder über den halbautomatischen Proxy-Modus für authentifizierte Seiten Swagger-Dateien lesen, die von Entwicklern geschrieben bzw. von der DenyAll WAF erzeugt wurden, wodurch Applikationsschwachstellen schneller aufgespürt werden können. Der Manager kann den Initialdeskriptor aktualisieren und ihn zur automatischen Validierung und für Virtuelles Patching an die DenyAll WAF weiterleiten.

5. **Monitoring und Reporting:** Eine tiefgreifende Untersuchung der umfassenden Protokolldaten der DenyAll WAF wird dank des konfigurierbaren DenyAll WAF Sicherheits-Dashboards, das auf Elastic Search und Kibana basiert, erheblich erleichtert. Manche Teams bevorzugen möglicherweise das vereinfachte mandantenfähige, anpassbare und rollenbasierte Benachrichtigungssystem, das den Datenverkehr ihrer Webapplikationen ebenso sichtbar macht.
6. **Weltweite Bereitstellung und Caching:** Der automatisierte WAF-as-a-Service wurde aufgrund des Inputs von großen und mittelgroßen Kunden weiterentwickelt. Sie beinhaltet nun Content-Delivery-Network-Features; die Regeln können granular konfiguriert werden und es bestehen individuelle Anpassungsmöglichkeiten, was die Arbeit von Webadministratoren erheblich erleichtert.

Mehr Sicherheitseffizienz durch die Verknüpfung der bisherigen Lösungen

Die DenyAll WAF beinhaltet ab sofort verschiedene Sicherheitsinstrumente, die ursprünglich in DenyAll rWeb, die frühere WAF des Unternehmens, beinhaltet waren. Administratoren können zusätzlich zu einer Normalisierungs-Engine, die helfen kann, WAF-Ausweichversuche zu vermeiden, auch auf die heuristische Engine von Scoring List zugreifen, um Zero-Day-Angriffe zu identifizieren. Darüber hinaus stehen Administratoren mit SQLi Sec und PathSec auch zwei hochentwickelte Erkennungs-Engines zur Verfügung, die durch Grammatikanalyse eine höhere Sicherheitseffizienz erreichen, was bei der Mehrzahl der kritischen Webapplikationen und Webservices von Vorteil ist. Deshalb ist die DenyAll WAF 6.3 eine solide Alternative für derzeitige rWeb-Kunden.

Live-Webinar

Nehmen Sie an unserem Webinar am 30. März 2017 um 11:00 Uhr MEZ teil, um eine Live-Vorstellung der neuen Features und der Vorteile, die sie für Ihre DevOps-Teams bereithalten, zu bekommen. Kunden und Partner können sich unter https://www.denyall.com/blog/events/webinar-automate-application-security-continuous-delivery/ für das Webinar anmelden.

DenyAll

Ein Unternehmen der Rohde & Schwarz Cybersecurity. Der europäische Marktführer für Web-Application-/Services-Security, DenyAll, ermöglicht nahtlose und sichere Nutzerinteraktion und unterstützt so Unternehmen bei der digitalen Transformation. Die Cloud-Dienste und Appliances von DenyAll erleichtern die Arbeit von Sicherheits- und DevOps-Teams über den gesamten Prozess der Software-Entwicklung hinweg und unterstützen sie bei der Schaffung einer sicheren digitalen Umgebung. Die Produkte tragen zur Erkennung, Priorisierung und Behebung von Schwachstellen bei. Sie machen die Verbindung zu Applikationen einfacher und sicherer für die Nutzer, unabhängig davon, wo sich Nutzer und Applikationen befinden. Darüber hinaus wehren sie Angriffe auf Webapplikationen, APIs und mobilen Apps zugrundeliegende Webdienste ab, indem sie das Nutzerverhalten kontextbasiert evaluieren und entsprechend reagieren. Mit den DenyAll-Lösungen für Applikationssicherheit der nächsten Generation können Sie die digitale Sicherheit Ihrer Nutzer sicherstellen. Erfahren Sie mehr unter www.denyall.com und www.cloudprotector.com.

Rohde & Schwarz Cybersecurity

Das IT-Sicherheitsunternehmen Rohde & Schwarz Cybersecurity schützt Unternehmen und öffentliche Institutionen weltweit vor Cyberangriffen. Mit hochsicheren Verschlüsselungslösungen, Next-Generation-Firewalls sowie Software für Netzwerkanalyse und Endpoint-Security entwickelt und produziert das Unternehmen technisch führende Lösungen für die Informations- und Netzwerksicherheit. Das Angebot der mehrfach ausgezeichneten und zertifizierten IT-Sicherheitslösungen reicht von kompakten All-in-one-Produkten bis zu individuellen Lösungen für kritische Infrastrukturen. Im Zentrum der Entwicklung von vertrauenswürdigen IT-Lösungen steht der Ansatz „Security by Design“, durch den Cyberangriffe proaktiv statt reaktiv verhindert werden. Knapp 450 Mitarbeiter sind an den derzeitigen Standorten in Berlin, Bochum, Darmstadt, Hamburg, Leipzig, München, Saarbrücken, Paris und Montpellier tätig.

Pressekontakte	
DenyAll GmbH Thomas Kohl Tel.: +49 170 161 32 50 tkohl@denyall.com www.denyall.com **Moeller PR** Eva Wagenbach Tel.: +49 221 801087 89 ew@moeller-pr.de	**DenyAll** Stéphane de Saint Albin Tel.: +33 1 46 20 96 21 sdesaintalbin@denyall.com www.denyall.com **Rohde & Schwarz Cybersecurity** Esther Ecke Tel.: +49 681 95986 212 cybersecurity@rohde-schwarz.com
