Pressemeldung

**BSI erteilt genugate 10.0 VS-NfD-Zulassung**

**High Resistance Firewall unterstützt IT-Konsolidierung mit neuen Automatisierungs-Features**

Kirchheim bei München, 16. März 2022. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die High Resistance Firewall genugate 10.0 Z für die Geheimhaltungsgrade „Verschlusssachen – nur für den Dienstgebrauch“ (VS-NfD), RESTREINT UE/EU RESTRICTED sowie NATO RESTRICTED zugelassen1. Diese aktuelle Version der IT-Sicherheitslösung unterstützt ab sofort eine REST-API sowie die zentrale Log-Auswertung über Elastic Stack. Staatliche Einrichtungen sowie Unternehmen mit sehr hohem Schutzbedarf können damit Administrationsaufgaben umfassend automatisieren, IT-Infrastrukturen weiter konsolidieren und gleichzeitig sensible Infrastrukturen zuverlässig gegen Cyber-Risiken absichern.

**Automatisierte Verwaltung komplexer Firewall-Systeme**

Technologie-Trends wie Cloud-Dienste, Remote-Anbindung oder die IT-Konsolidierung erhöhen auch im öffentlichen Sektor die Komplexität von IT-Systemlandschaften. Dies erschwert es IT-Administratoren zunehmend, Firewalls effizient zu verwalten und zu kontrollieren. Damit steigt auch das Risiko für Fehlkonfigurationen und Sicherheitslücken.

Um aufwändige Administrationsaufgaben über eine große Zahl von Appliances zuverlässig zu handhaben, unterstützt die neue Version 10.0 Z der genugate eine REST-API, die eine maschinenlesbare Definition nach dem OpenAPI-Standard bietet. Behörden und Unternehmen können die Firewall so in großem Maßstab einsetzen und Prozesse einfach und transparent automatisieren. Hierzu zählen das Anlegen von Host-Einträgen, der Abgleich von Regelwerken über mehrere Installationen, die Erstellung von Regeln zur Einbindung in eine Cloud-Infrastruktur oder die Regelwerksdokumentation für Audit-Zwecke.

**Verbesserte Auswertung und Analyse von Log-Meldungen**

Die genugate 10.0 Z unterstützt außerdem ein zentrales Logging über Elastic Stack. Die Anbindung an die auch als ELK-Stack bekannte Open-Source-Lösung erlaubt eine komfortable Auswertung, Analyse und Behandlung von Log-Meldungen mehrerer Firewalls über eine einzige Benutzerschnittstelle (GUI) sowie das Echtzeit-Monitoring sicherheitskritischer Funktionen. So lassen sich selbst bei hochkomplexen Systemen mit vielen Devices Warnmeldungen schnell lokalisieren, bewerten und Maßnahmen ableiten.

Web Application Security und sichere Software-Updates

Die genugate 10.0 Z ist ferner weltweit die einzige Web Application Firewall (WAF), die durch das BSI eine Zertifizierung nach Common Criteria (CC) EAL4+ mit AVA\_VAN.5 (Advanced Methodical Vulnerability Analysis) erhalten hat. Die Bezeichnung AVA\_VAN.5 steht für ein hohes Maß an Selbstschutz, durch den die Firewall nachweislich selbst Angreifern mit hohem Angriffspotential standhält. Besonders gefährdete Organisationen wie Sicherheitsbehörden, Militär oder Betreiber kritischer Infrastrukturen können somit ihre Server zuverlässig vor Angriffen schützen.

Als einzige Firewall am Markt verfügt genugate 10.0 Z außerdem über ein nach CC EAL4+ zertifiziertes Patch-Management. Dieses sorgt zusätzlich für einen besonders effektiven Schutz von Software-Maintenance-Prozessen wie Updates und Patches gegen Infiltrationsversuche.

1IT-Sicherheitsprodukte, die innerhalb von Verschlusssachen-IT (VS-IT) im Behördenumfeld Sicherheitsfunktionen übernehmen, sind vor ihrem Einsatz vom BSI zuzulassen. Die aktuelle BSI-Zulassung für genugate 10.0 Z ist gültig bis zum 2. Februar 2024.

**Bildunterschrift**

genugate ist eine High Resistance Firewall, die ein Application Level Gateway und einen Paketfilter, jeweils auf separater Hardware, zu einer kompakten Lösung vereint. Durch ihre Zweistufigkeit und einen hohen Selbstschutz bietet die Appliance ein besonders hohes Sicherheitsniveau.

© genua GmbH

**Weitere Informationen**

* Produktinformationen zur High Resistance Firewall genugate https://www.genua.de/genugate
* Firewall- und Gateway-Lösungen von genua https://www.genua.de/it-sicherheitsloesungen/firewalls-gateways

**Über genua**

Die genua GmbH ist Enabler der digitalen Transformation. Wir sichern sensitive IT-Netzwerke im Public- und im Enterprise-Sektor, bei KRITIS-Organisationen und in der geheimschutzbetreuten Industrie mit hochsicheren und skalierbaren Cyber-Security-Lösungen. Dabei fokussiert sich die genua GmbH auf den umfassenden Schutz von Netzwerken, Kommunikation und interner Netzwerksicherheit für IT und OT. Das Lösungsspektrum umfasst Firewalls und Gateways, VPNs, Fernwartungssysteme, interne Netzwerksicherheit und Cloud Security bis hin zu Remote-Access-Lösungen für mobile Mitarbeiter und Home Offices.

Die genua GmbH ist eine Tochtergesellschaft der Bundesdruckerei-Gruppe. Mit mehr als 350 Mitarbeitern entwickelt und produziert sie IT-Security-Lösungen ausschließlich in Deutschland. Seit der Unternehmensgründung in 1992 belegen regelmäßige Zertifizierungen und Zulassungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) den hohen Sicherheits- und Qualitätsanspruch der Produkte. Zu den Kunden zählen u.a. Arvato Systems, BMW, die Bundeswehr, das THW sowie die Würth-Gruppe.

Pressekontakt

genua GmbH

Martina Hafner

Presse & PR

T +49 171 56 92 523

E martina\_hafner@genua.de