



# Worauf es bei Firewalls für Kommunen ankommt



Für den IT-Administrator einer bayerischen Gemeinde sind bei der Auswahl einer Firewall-Lösung vor allem fünf Kriterien entscheidend: Eine nachweisbare, also zertifizierte Sicherheit; eine auch für Nicht-IT-Security-Experten gute Bedienbarkeit; die Tauglichkeit für den IT-Alltag; eine vertrauenswürdige Lösung Made in Germany und schließlich ein zuverlässiger und gut erreichbarer Support.

Kommunen und öffentliche Verwaltungen stehen beim Thema IT-Sicherheit oft unter mehrfachem Druck. Sie haben mit Einwohnermeldedaten, Gewerbesteuerbescheiden oder den Finanzdaten der Gemeinde eine große Menge an besonders schützenswerten Informationen und haben dennoch nur begrenzte Ressourcen zum Schutz der Daten. „Wir haben nach einer Firewall-Lösung gesucht, die technisch höchste Sicherheit garantiert und gleichzeitig mit nur geringem Administrationsaufwand bedienbar und alltagstauglich ist“, fasst Andreas Pecher, IT-Administrator der oberbayerischen Gemeinde Kirchheim bei München, seine Anforderungen zusammen. Dabei nehmen die Ansprüche der internen Fachan-

wender als auch die Herausforderungen durch neue digitalisierte Dienstleistungen aus dem E-Government kontinuierlich zu.

Kirchheim kann mit seinen etwa 13.000 Einwohnern und seinen kurzen Wegen zur Messe München, zum Flughafen oder in die Landeshauptstadt sowohl auf steigende Einwohnerzahlen als auch auf einen gesunden Branchenmix verweisen. Die Größe der Gemeinde lässt jedoch nicht die Beschäftigung von IT-Securityspezialisten zu, sodass der IT-Administrator für alle IT-Themen zuständig ist. „Bei komplexeren IT-Security-Problemen hätte ich gar nicht die Zeit, mich in die letzten technischen Details zu vertiefen.



## High Resistance Firewall genugate: Zweistufige Sicherheitslösung mit BSI-Zertifikat



Deshalb war sowohl bei der Installation als auch beim Support die kompetente Unterstützung des Firewall-Herstellers ein Entscheidungskriterium“, so Andreas Pecher.

### BSI-zertifizierte Firewall „Made in Germany“

Die alte Firewall der Gemeinde war seit Jahren im Einsatz und inzwischen völlig unterdimensioniert. Bei der Auswahl einer neuen Lösung hatte der IT-Administrator etliche Herstellerangebote verglichen. „Wir haben uns schließlich für die Firewall genugate des deutschen Herstellers genua entschieden, weil diese Lösung unsere Anforderungen am besten erfüllt. Besonders die Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik war uns sehr wichtig, da auf diesen Aspekt auch der kommunale Prüfverband achtet“, erläutert Andreas Pecher den Stellenwert einer nachweisbaren, zertifizierten Sicherheit.

Vom Bundesamt für Sicherheit in der Informationstechnik (BSI) werden Prüfungen und Bewertungen der Sicherheit von Informationstechnik nach internationalen ISO-/IEC-Standards (Common Criteria) durchgeführt. Die genugate ist die einzige Firewall weltweit, die die BSI-Zertifizierung in der Stufe EAL 4+ mit dem Prädikat „Highly Resistant“ vorweisen kann, weil sie direkten

Angriffen nachweisbar höchsten Widerstand entgegengesetzt.

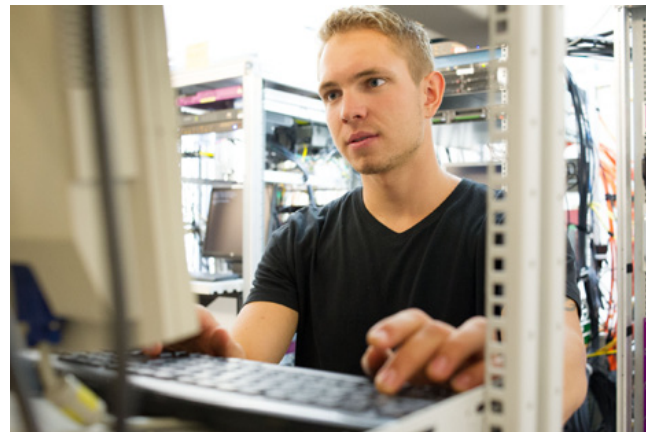
„Die Kombination aus einer BSI-zertifizierten Sicherheit, bei der auch der komplette Quellcode vorgelegt werden muss und einer zweistufigen, Hardware-basierten Firewall-Technik aus Deutschland ist überzeugend“, fasst der IT-Administrator die Gründe zusammen.

### Zweistufige Firewall-Lösung

Die Lösung von genua besteht aus den beiden Stufen „Application Level Gateway“ (ALG) und „Paketfilter“. Mit der ersten Komponente wird der komplette Inhalt des Datenstroms analysiert und auf gefährliche oder unerwünschte Inhalte gründlich untersucht. Dazu werden die ankommenden Datenpakete zunächst gestoppt – das ALG lässt keine durchgehende Verbindung zwischen Internet und lokalem Netz zu. Dadurch werden Angriffe auf der Netzebene verhindert und Risiken beispielsweise durch die erweiterten Header bei IPv6 ausgeschlossen. Die eintreffenden IP-Pakete werden zunächst zu ganzen Datensätzen zusammengesetzt, damit sie überhaupt überprüfbar werden. Prüfprogramme für alle gängigen Protokolle sowie ein Virens Scanner analysieren dann den Inhalt der empfangenen Daten. Aktiver Content, Viren oder Spam werden hier zuverlässig erkannt und abgeblockt. Ist die



## Die Firewall genugate bietet viele Möglichkeiten, um den Empfang bestimmter Dateitypen oder Inhalte zu beschränken oder auszuschließen.



Inhaltsprüfung bestanden, erzeugt das ALG eine neue Verbindung und schickt die Datenpakete zum zweiten Firewall-System, dem Paketfilter.

Der Paketfilter prüft als weiteres Firewallsystem die Datenpakete auf der formalen Ebene: Absender- und Empfängeradresse, Protokolltyp etc. Nur wenn die Verbindung gemäß den konfigurierten Regeln erlaubt ist, leitet der Paketfilter die Daten an den Empfänger weiter. Somit ergänzen sich ALG und Paketfilter auf verschiedenen Ebenen und erreichen so die hohe Sicherheitsleistung.

### Mehr als Deep Packet Inspection

Der Firewall-Hersteller genua betont den Unterschied zu herkömmlichen Deep Packet Inspection oder Next Generation Firewalls. Bei genugate werde Wert auf eine hohe Performance gelegt. Noch wichtiger sei aber die vollständige und korrekte Analyse des gesamten Datenstroms – im Unterschied zu den Stichprobenkontrollen anderer Hersteller. So werde besonders bei verschleierte Dateiformaten und auch bei zweifelhaften URL- und IP-Quellen detailliert geprüft. Untersucht wird auch die Korrektheit von Zertifikaten. Zudem werden auch zip-komprimierte Dateien oder verschlüsselte https-Verbindungen genauestens kontrolliert.

Dem Anwender stehen in der Firewall außerdem etliche Konfigurationsmöglichkeiten zur Verfügung, um beispielsweise den Empfang bestimmter Dateitypen oder Inhalte wie Java-Skript, Audio- oder Medien-Dateien ganz oder zeitlich beschränkt auszuschließen. „Bei der Lösung wird der Vorteil einer reinen IT-Security-Firma sofort deutlich. Das gesamte Konzept ist sehr stimmig und eine zweistufige, Hardware-basierte Lösung ist in dieser Preiskategorie sonst kaum zu finden“, ergänzt der IT-Administrator den Preis-Leistungs-Aspekt.

### Support von einem deutschen Hersteller

Die Gemeinde Kirchheim musste bei der Einführung der Firewall-Lösung vor allem die Migration von der alten Lösung sowie die Integration zahlreicher Schnittstellen zu Fachverfahren berücksichtigen. Der IT-Administrator hebt hier die Beratung und die gute Schulung von genua vor der Einführung sowie die Unterstützung bei der Installation hervor. Das habe ihm sehr geholfen, die große Zahl kleiner Baustellen überhaupt zu bewältigen. „Es ist schon ein Riesenunterschied, ob ich einen Lieferanten aus einer anderen Zeitzone oder einen deutschen Hersteller mit einem fachlich überzeugenden Support habe“, bilanziert Andreas Pecher die Vorbereitungs- und



Einführungsphase. Der Hersteller genua gibt in seinem Unternehmensblog außerdem hilfreiche Tipps und Hinweise aus dem IT-Security-Umfeld. (<https://blog.genua.de>)

Die Firewall genugate ist bei der Gemeinde jetzt seit eineinhalb Jahren im Betrieb. Der IT-Administrator verweist auf die alltagstaugliche Anwendbarkeit der Lösung. Deshalb sei die gut nachvollziehbare Bedienbarkeit der Administrations-Oberfläche entscheidend: „Die Firewall macht immer genau das, was man ihr sagt. Auch nach eineinhalb Jahren Betrieb hatten wir noch kein Problem.“

Die bayerische Staatsregierung hat ein Förderprogramm zu ISIS12 aufgelegt. Kommunen werden unterstützt, wenn Sie ein IT-Sicherheitsmanagement gemäß dem ISIS12-Modell einführen. Dazu gehört auch der Einsatz von Firewalls, die vollständig nach Common Criteria mindestens in der Stufe EAL 4 zertifiziert sind. Die Firewall genugate erfüllt diese Anforderung.

**Infos zu dem Programm:**

<https://www.it-sicherheit-bayern.de/produkte-dienstleistungen/isis12.html>



Autor: *Martin Ortgies*,  
Technikjournalist aus Hannover

Weitere Informationen unter:  
[www.genua.de/genugate](http://www.genua.de/genugate)