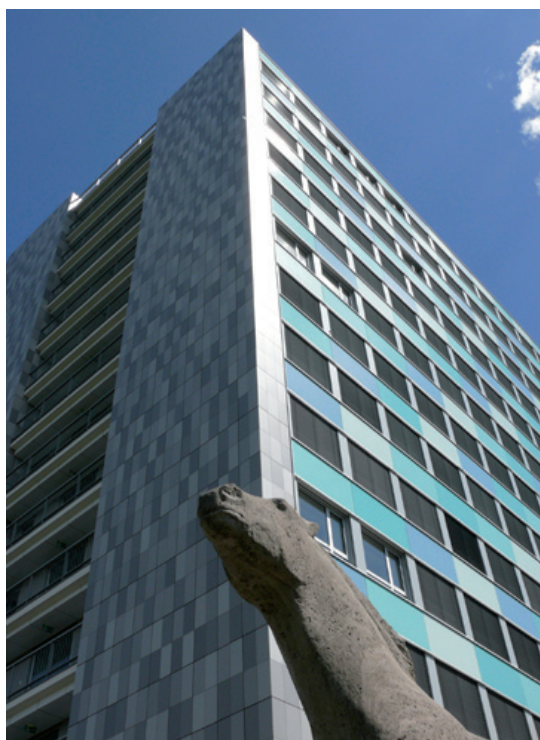




# Firewalls sichern Ergebnis der Bundestagswahl

**DESTATIS**  
wissen.nutzen.



## Bundesamt schützt Webserver mit Firewall-Cluster von GeNUA

Bei jeder Bundestags- und Europawahl kommt es bei Destatis (Statistisches Bundesamt) zu einem massiven Ansturm aus dem Internet. Sobald die ersten Stimmen gezählt sind, laufen die Ergebnisse aller Wahlkreise bei dem Amt in Wiesbaden zusammen und werden auf der Webseite des Bundeswahlleiters veröffentlicht. Hierauf wird innerhalb kurzer Zeit sehr häufig zugegriffen – bei der Bundestagswahl 2005 wurden in der Spitze fast 1,4 Millionen Hits pro Stunde gezählt. Auf diese besondere Situation musste die IT auch für die Bundestagswahl 2009 vorbereitet werden: Destatis installierte hierfür mehrere zusätzliche Server mit je drei Webserver-Instanzen und davor eine Phalanx zertifizierter Firewalls mit Load Balancing-Funktion, um alle Anfragen ohne Downtime möglichst schnell zu bedienen und die Webseiten vor Manipulationen zu schützen.

Der Präsident von Destatis ist zugleich Bundeswahlleiter in Deutschland. Wahlen zum Bundestag und Europäischen Parlament werden von ihm organisiert und überwacht. Schließlich verkündet er auch das amtliche Ergebnis. Am Wahltag hält sich der Präsident dazu im Berliner Reichstag auf, aber bei der Informationstechnik (IT) laufen die Fäden an seinem Wiesbadener Dienstsitz zusammen: Die Ergebnisse aller Wahlkreise werden von den Landeswahlleitern hierhin digital gemeldet, aufbereitet und auf die Webserver gestellt,

auf die unter [www.bundeswahlleiter.de](http://www.bundeswahlleiter.de) zugegriffen werden kann. Und diese Zugriffe erhöhen sich in der Wahlnacht gewaltig. Bei der Bundestagswahl im September 2005 gab es innerhalb von 36 Stunden über 12,6 Millionen Hits auf diese Webseite.

## **Bundestagswahl 2009: Starker Ansturm auf Webserver erwartet**

Als am 27. September 2009 die nächste Bundestagswahl anstand, erwartete die IT-Abteilung von



Destatis einen noch stärkeren Ansturm aus dem Internet. Interne Schätzungen rechneten im Extremfall mit der fünf- bis sechsfachen Anzahl an Zugriffen innerhalb der ersten 36 Stunden nach Schließung der Wahllokale gegenüber 2005. Darauf musste die IT vorbereitet werden. Um deutlich mehr Internet-Anfragen bearbeiten zu können, installierten die Administratoren mehrere zusätzliche Server. Die weitere Aufgabenstellung war, diese Server gegen unbefugte Zugriffe und Manipulationen zuverlässig abzusichern und die große Anzahl an Anfragen gleichmäßig zu verteilen, um möglichst kurze Antwortzeiten zu erreichen. Gefordert waren also ein vorgeschaltetes Firewall-System und eine Load Balancing-Lösung, um jeden Zugriffe aus dem Internet zu kontrollieren und dann an einen Server mit freier Kapazität weiterzureichen.

Die Aufgabe wurde mit Firewalls des deutschen Herstellers GeNUA gelöst. Dessen Firewall GeNUScreen kennzeichnet die Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Das Problem: IT-Sicherheitssysteme wie Firewalls sind so komplex, dass es für die Anwender nicht möglich ist, die Qualität der Lösungen zu beurteilen. Ist die Firewall tatsächlich ganz sauber programmiert, keine Schwachstelle oder Hintertür enthalten und wird die versprochene Sicherheitsleistung erbracht?

### **BSI-Zertifizierung als Qualitätsnachweis**

Bei einer Zertifizierung nach einem anerkannten Standard werden die Aussagen des Herstellers von unabhängigen Experten übergeprüft; je höher die angestrebte Stufe, desto tiefer gehen die Analysen. GeNUA hat die Firewall GeNUScreen beim BSI nach dem internationalen Standard Common Criteria (CC) in der Stufe EAL 4+



**Präsident des Destatis und Bundeswahlleiter:  
Roderich Egeler**

zertifizieren lassen. Dies ist die höchste Stufe, die auf ein komplexes Firewall-System anwendbar ist, und beinhaltet umfassende Analysen bis hinunter zum Quellcode und ausführliche Testverfahren. Durch die erfolgreiche Zertifizierung haben Anwender von unabhängiger Seite die Gewähr, dass die Sicherheitsfunktionen korrekt umgesetzt sind und leisten, was der Hersteller verspricht.

Ein weiteres Merkmal der Firewall GeNUScreen ist die Möglichkeit, mehrere Systeme zu einem Cluster zu verbinden: Die parallel geschalteten Firewalls teilen sich die Arbeit und übernehmen bei einem Ausfall sofort die Aufgaben des Partner-Systems. So wird eine leistungsstarke und ausfallsichere Verbindung garantiert. Zusätzlich zu den Sicherheitsmechanismen bietet die



Firewall auch eine Load Balancing-Funktion. Diese ist in das Betriebssystem OpenBSD integriert, das zusammen mit der Firewall-Software und der zugrunde liegenden Hardware die Appliance GeNUScreen bildet. Wird die Load Balancing-Funktion aktiviert, dann behält die Firewall die Auslastung der Zielsysteme im Blick und sendet neue Anfragen stets an den Server, der gerade am wenigsten zu tun hat. So werden möglichst kurze Antwortzeiten erreicht und eine Überlastung der Server vermieden. Diese Funktionen erfüllten somit die gestellten Anforderungen, deshalb entschied sich die IT-Abteilung von Destatis zu einem Einsatz der Firewall GeNUScreen.

### **Vier Firewalls vor mehreren Webservern**

Nach der Produktauswahl war zu klären, wie viele Firewalls erforderlich sind, um die Anfragen verzögerungslos zu bearbeiten. Nach erster Teststellung, die auch für die Durchführung der Europawahl im Juni 2009 genutzt wurde, entschied Destatis, vier Firewalls des Typs GeNUScreen 400 vor die physikalischen Webserver zu stellen, auf denen je drei Webserver-Instanzen parallel liefen. Die vier Firewalls wurden zu einem ausfallsicheren Cluster verbunden, um mit hoher Performance die Anfragen aus dem Internet zu filtern. Die zulässigen Zugriffe wurden dann mit Load Balancing auf die vielen dahinter stehenden Webserver verteilt und die Antworten schließlich wieder an den Sender zurückgeschickt. Bei der

Installation unterstützte der Hersteller die Administratoren von Destatis; konfiguriert und verwaltet wurden die Firewalls über ein zentrales Management System mit übersichtlicher Benutzeroberfläche.

Als am 27. September 2009 abends die Wahllokale schlossen, stieg die Last auf den Firewalls und den Webservern rapide an: Die höchste Zugriffszahl pro Stunde lag bei fast 3,9 Millionen Hits, insgesamt wurden über 32,6 Millionen Hits innerhalb der ersten 36 Stunden registriert. Alle Anfragen wurden dabei von den Firewalls und den Servern ohne Downtime oder längere Wartezeiten bearbeitet.

### **Das Fazit von Destatis:**

*Die Lösung funktionierte gut unter der großen Last. Auch die Vorbereitungen für den Produktionsbetrieb – Installation und Konfiguration – gingen mit Unterstützung des Herstellers zügig voran. Die Lösung hinterließ insgesamt einen guten Eindruck und hat sich auch für kommende, größere IT-Projekte empfohlen.*