



Stadt Mülheim setzt auf zweistufige Firewall GeNUGate

Mit Anti-Spam-Funktion Greylisting 95 Prozent des lästigen Datenmülls abgeblockt

Städte sind große Dienstleister: Ausweise müssen ausgestellt, die Straßen gereingt, Wahlscheine zugeschickt, der Sperrmüll abgeholt, Bauanträge bearbeitet und Aufenthaltsgenehmigungen erteilt werden. Dies ist nur ein Auszug aus dem breiten Leistungsspektrum, dass für die Bürger schnell und einfach abrufbar sein soll. Damit ist klar: Möglichst viele Leistungen sollten online bestellt werden können – am besten interaktiv mit direkter Anbindung an das Rathaus. Für diese Bürgernähe sind Schnittstellen zwischen Internet und städtischem Netzwerk erforderlich, die jedoch zuverlässig geschützt werden müssen. Denn Stadtverwaltungen arbeiten mit einer Menge sensibler Informationen.



Die Stadt Mülheim an der Ruhr bietet komfortablen Online-Service



Die Stadt Mülheim an der Ruhr ist diesen Weg weit gegangen. Über ihren Internet-Bürgerservice können eine Vielzahl von Behördengängen direkt online abgewickelt werden. Ausgehend vom Wunsch der Bürger verwendet die Stadt Mülheim an der Ruhr überwiegend „echte“ Online-Formulare, die unmittelbar am Bildschirm ausgefüllt und abgesandt werden können. Dieser komfortable Service erspart den Mülheimern immer öfter den Gang ins Rathaus. Die moderne Verwaltung der „Stadt am Fluss“ nutzt das Internet auch für den schnellen Datenaustausch mit anderen Behörden, beispielsweise für elektronische Steuererklärungen an die Oberfinanzdirektion oder Mitteilungen an das Kraftfahrt Bundesamt in Flensburg. Zusätzlich haben rund 1.450 städtische Mitarbeiter Zugriff auf das WWW.

Täglich Portscans von Hackern auf der Suche nach Schwachstellen

Diese effizienten Abläufe ermöglichen kurze Bearbeitungszeiten, stellen jedoch auch hohe Anforderungen an die IT-Sicherheit. Denn der Informationsaustausch der Stadt Mülheim über das Internet summiert sich inzwischen auf rund 100 Gbit pro Monat, und jedes Datenpaket muss gründlich kontrolliert werden. Die Gefahr in Zahlen: Täglich registriert die städtische Systemverwaltung durchschnittlich vier Portscans, also Hacker auf der Suche nach Schwachstellen in der Netzwerk-Absicherung. Dazu kommen zahlreiche schädliche Datenpakete, die vom Virenschanner herausgefischt werden müssen. „Wir gehen mit vielen hochsensiblen Daten um, Informationen über jeden einzelnen gemeldeten Einwohner oder Daten über gewährte Sozialleistungen sind nur einige Beispiele. Hier tragen wir hohe Verantwortung und müssen unser Netz sehr sorgfältig absichern“, erläutert Joachim A. Lühr, System- und Netzwerkadministrator der Stadtverwaltung Mülheim an der Ruhr.

Zweistufige Firewall mit Application Level Gateway und Paketfilter

Mülheim schützt das Netzwerk an der kritischen Nahtstelle zum Internet mit der Firewall GeNUGate, einer Lösung des auf IT-Sicherheit spezialisierten Unternehmens GeNUA. Das Besondere an diesem System:



Die GeNUGate vereint zwei Firewalls – ein Application Level Gateway und einen Paketfilter – in einer Lösung. Auf dem Weg vom Internet zum städtischen Netzwerk müssen Daten beide Firewalls passieren und werden ausführlich überprüft.



Firewall GeNUGate mit Application Level Gateway und Paketfilter

Kernstück der Firewall-Lösung ist das Application Level Gateway. Dieses Sicherheitssystem prüft den Inhalt des Datenstroms. Dazu werden die ankommenden Datenpakete zunächst gestoppt – das Application Level Gateway lässt niemals eine durchgehende Verbindung zwischen Internet und Netzwerk zu. Dann setzt es die einzelnen Pakete wie ein Puzzle zusammen, denn nur anhand kompletter Datensätze ist eine inhaltliche Prüfung möglich. Jetzt wird gefiltert: WWW-Daten auf Viren und auf aktive Inhalte, von denen nur ausdrücklich über Whitelisting zugelassene Javascripte durchgelassen werden. Emails werden ebenfalls auf Viren gescannt, zusätzlich nach Blocked Pattern inhaltlich auf Spam durchforstet.

Greylisting: neues Verfahren gegen Datenmüll

Gegen den unerwünschten Datenmüll bietet die GeNUGate seit dem Release-Wechsel im Herbst 2004 mit Greylisting ein weiteres, neuartiges Verfahren. Greylisting basiert auf einem einfachen Trick: Bei jeder eingehenden Email werden die drei Informationen IP-Adresse des sendenden Mails-



Servers, Absender- sowie Empfängeradresse abgefragt. Wenn diese Dreier-Kombination zum ersten Mal vorkommt, wird die Email abgewiesen, das neue Triple jedoch gespeichert. Seriöse Mail-Server unternehmen in diesem Fall gemäß dem RFC-Standard nach kurzer Zeit einen zweiten Zustellversuch. Jetzt ist die Dreier-Kombination bereits bekannt, die Post wird zum Empfänger durchgelassen. Spammer setzen dagegen auf Masse innerhalb möglichst kurzer Zeit und möchten sich nicht mit wiederholten Zustellungen aufhalten. Sie arbeiten deshalb fast immer nach der Methode „fire and forget“ - und scheitern damit am Greylisting.

95 Prozent weniger Spam

Kommunikationsprobleme entstehen lediglich zu seriösen Mail-Servern, die nicht RFC-konform arbeiten. Dies sind jedoch nur wenige, und sie können von diesem Verfahren ausgenommen werden. „Greylisting ist sehr effektiv, bei uns kommt 95 Prozent weniger Spam an. Damit ist dieses lästige Problem praktisch gelöst“, resümiert Joachim A. Löhr nach einem halben Jahr Spam-Kontrolle mit grauen Listen.



Alles sicher: Blick auf Mülheim von der Ruhr aus



Zweite Prüfung: Paketfilter kontrolliert formale Kriterien

Nach dieser sorgfältigen Inhaltskontrolle leitet das Application Level Gateway die Daten weiter an den Paketfilter. Er prüft die Pakete auf der formalen Ebene: Sind die Absenderadresse, der verwendete Protokolltyp sowie die angesteuerte Port-Nummer zugelassen? Erst wenn auch diese Prüfung bestanden ist, wird das empfangene Paket in das Netz der Stadt Mülheim durchgelassen.

Die Firewalls haben noch nie Sicherheitsprobleme zugelassen

Die Stadtverwaltung Mülheim setzt seit 1997 die Firewall GeNUGate ein, 2003 wurde die Lösung mit einem zweiten System zu einem hochverfügbaren Cluster aufgerüstet. „Die GeNUGate mit zwei aufeinander abgestimmten Firewalls, deren Kontrollmechanismen sich auf unterschiedlichen Ebenen ergänzen, bietet zuverlässigen Schutz für unser Netzwerk. Die Lösung hat noch nie Sicherheitsprobleme zugelassen“, so Joachim A. Löhr. Diese Einschätzung bestätigt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Es hat die zweistufige Lösung nach dem internationalen Standard ITSEC in der Stufe E3 hoch zertifiziert. Die GeNUGate ist die einzige Firewall-Lösung, die vom BSI mit diesem Qualitätssiegel ausgezeichnet wurde.