circular

SICHER GEGEN DDOS-ATTACKEN

Schnelles und ausfallsicheres Internet für die baden-württembergische Wissenschaft

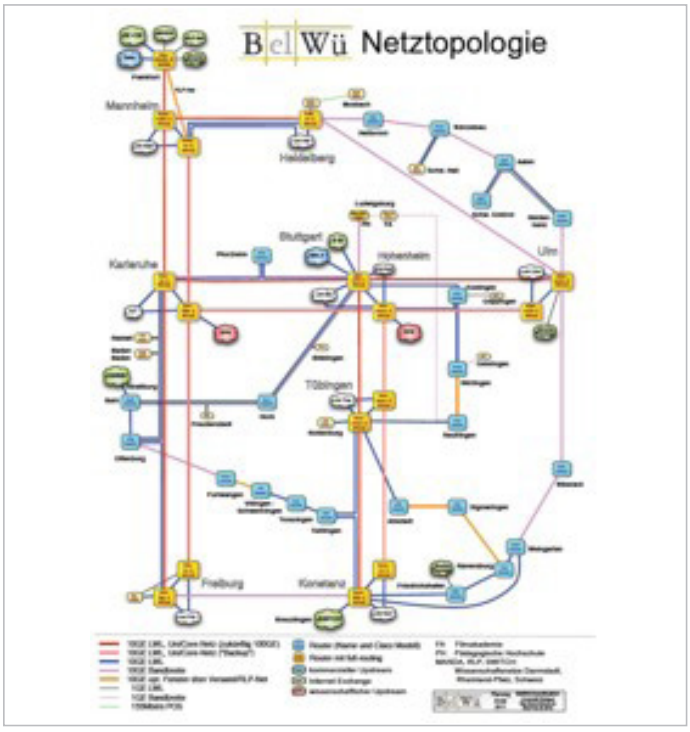
BelWü
Landeshochschulnetz Baden-Württemberg

Unternehmen	Universität Stuttgart BelWü-Koordination
Branche	Wissenschaft
Land	Deutschland
Website	www.belwue.de

„Wir können zwar kein Hochdeutsch – aber Forschung und Lehre." Mit zwölf Graduiertenschulen, sieben Exzellenzclustern und überzeugenden Zukunftskonzepten, laut der sogenannten Exzellenzinitiative, ist die baden-württembergische Hochschullandschaft bestens im deutschen Ländervergleich aufgestellt. Zu einem erfolgreichen Bildungssystem gehört jedoch auch eine stabile, schnelle und sichere IT-Landschaft: Das Baden-Württemberg extended LAN, kurz **BelWü**, ist solch eine Infrastruktur und **verbindet** die **neun Landesuniversitäten**, über **25 Hochschulen**, die **Duale Hochschule Baden-Württemberg** mit **acht Standorten** und **vier Campusse** sowie andere wissenschaftliche Einrichtungen über schnelle Datenleitungen untereinander. Dieses wichtige Netzwerk muss natürlich geschützt werden. Deswegen hat die circular Informationssysteme GmbH gemeinsam mit ihrem Partner Arbor Networks die BelWü-Anwendungen noch sicherer gegen DDoS-Attacken gemacht.

Geschäftsbedarf

Hauptaufgabe des Hochschulnetzes BelWü ist die extrem **schnelle Verbindung** der Wissenschaftseinrichtungen in Baden-Württemberg – primär der Universitäten untereinander – an das öffentliche Internet. Grundlage hierfür sind angemietete Glasfasern, über die ein Netzwerk mit Hilfe leistungsfähiger Cisco-Router gebildet wird. **Baden-Württemberg** hat als **einziges Bundesland** solch ein **schnelles Datennetz**, das auch kleinere Institutionen, wie Schulen oder Bibliotheken, mit extrem schnellen Anbindungen versorgt. Diese können sich per DSL, Wähl- oder Festverbindung an das Netz anschließen.



Darüber hinaus betreibt BelWü die leistungsfähige E-Learning-plattform Moodle für Schulen. Damit haben beispielsweise Lehrer die Möglichkeit, Schülerinnen und Schülern online Materialien, Übungen und Kommunikationsmöglichkeiten in einem abgeschlossenen Kursraum zur Verfügung zu stellen. Dort können Projekte organisiert und das selbst gesteuerte Lernen gefördert werden.

„DAS SYSTEM- UND BERATUNGSHAUS HAT UNS EIN RUND-UM-PAKET GELIEFERT. ES STAND UNS MIT BERATUNG, BEI DER BESCHAFFUNG UND ERSTINSTALLATION SOWIE DER TESTSTELLUNG UND ERSTKONFIGURATION DER LÖSUNG ZUR SEITE."

Peter Merdian, Koordinator von BelWü

Größe verpflichtet zu Ausfallsicherheit

Der Zugriff durch Anwender auf zentrale Ressourcen, wie Supercomputer oder Bibliotheksdatenbanken, erfordert aufgrund der großen Datenmengen höchste Übertragungsraten. Außerdem werden extrem **ausfallsichere Netze**, wegen der Abhängigkeit von zentralen und über das Land verteilten Diensten und Datenbanken, im täglichen Betrieb benötigt. Vor allem die immer wichtiger werdenden Webserver müssen geschützt werden. Denn Ausfallszenarien und Gefahren gibt es viele, betrachtet man die zunehmenden Distributed-Denial-of-Service(DDoS)-Angriffe. Sollten Web, SMTP oder andere Dienste durch solche Attacken nicht mehr verfügbar sein, wird alles andere zur Nebensache.

Was sind DDoS-Attacken und was macht sie so gefährlich?

Ein DDoS-Angriff wird von vielen Rechnern aus dem Internet gestartet, die gleichzeitig dasselbe Ziel angreifen. Hierbei spielt es keine Rolle, ob dieser von infizierten „ferngesteuerten" Rechnern ausgeht oder es sich um eine abgesprochene Attacke von Personen handelt. Die Angriffe richten sich im Allgemeinen gegen Bandbreite, Applikationen und Verbindungsstatus. Meist wird der Angriff über ein Bot-Netz initiiert. Computer werden über Trojaner infiziert und zu sogenannten Zombies gemacht. Diese setzen sich dann mit dem Command- & Control-Server (C & C) des Angreifers in Verbindung. Über diesen Weg können die Zombie-Rechner ihre Erreichbarkeit übermitteln und/oder sich einen neuen Programmcode abholen. Der Betreiber des Command- & Control-Servers erlangt damit die Kontrolle über die fremden Computer-Zombies, die sie dann dazu nutzen, Angriffe zu starten oder Spam zu versenden. Bei einem DDoS-Angriff werden die Angriffssignaturen über den C&C-Server an die infizierten PCs weitergegeben, die dann ICMP-, TCP-Syn- oder andere Angriff auf die in der Signatur angegebene Zieladresse ausführen. Ziel einer DDoS-Attacke ist es, dass ein Netzwerk oder Dienst über das Internet nicht mehr erreichbar oder stark gestört ist.

Moderner Schutz gegen moderne Angriffsformen

Tatsächlich haben DDoS-Attacken in der Vergangenheit auch den BelWü-Betrieb mehrfach gestört. In den vergangenen zwei Jahren wurden zunehmend die Webserver angegriffen. Dadurch war deren Verfügbarkeit oft gefährdet. Generell haben sich DDoS-Attacken in den letzten Jahren stark verändert. Während früher die Infrastruktur der Serviceprovider stark betroffen war, werden heute in zunehmendem Maße Endkunden und ihre Applikationen angegriffen. Dies hat die baden-württembergische Organisation in Zusammenarbeit mit circular erkannt. Durch eine langjährige, gute Zusammenarbeit wurde von Seiten der BelWü von Anfang an Vertrauen in die **Security-Experten** von circular gesetzt. Das Projektteam bestand aus einem Projektleiter, Systemadministratoren und Netzwerkingenieuren vom BelWü. Unterstützt wurden diese Fachleute von einem Security-Consultant von circular. Zunächst wurde eine Beratung und Produktpräsentation durchgeführt. *Peter Merdian, Koordinator von BelWü:* „Das System- und Beratungshaus hat uns ein Rund-um-Paket geliefert. Es stand uns mit Beratung, bei der Beschaffung und Erstinstallation sowie der Teststellung und Erstkonfiguration der Lösung zur Seite. Danach wurden gleich die ersten Updates eingespielt. Innerhalb von vier Monaten konnte das Projekt erfolgreich beendet werden. Die vorgegebene Zeit wurde eingehalten."

Gefahren bannen per Mausklick

Verwendet wurden Produkte von Arbor Networks. Das **Pravail Availability Protection System (APS)** sorgt für eine gezielte Abwehr von Angriffen auf die Dienstverfügbarkeit von Rechenzentren und Datennetzen. Wird die Pravail APS Appliance diesen angreifbaren Diensten vorgeschaltet, können Rechenzentren Angriffe schnell auf Applikationsebene stoppen und Attacken aus Botnetzen unterbinden.

Tobias Löhnert, Webmaster bei BelWü, erklärt, wie die neue

Lösung im Detail funktioniert: „Auf unserem Router sind mehrere Virtual Local Area Networks – kurz VLANs – definiert, in denen jeweils die Interfaces der Arbor und die einzelnen Webserver hängen. Die Arbor-Lösung ist dabei auf der sogenannten Layer 3 zwar nicht sichtbar, verhält sich aber wie eine Bridge. Das bedeutet, sie lässt den Datenverkehr jeweils von Interface zu Interface durchlaufen und inspiziert den gesamten Traffic." Ein manuelles Eingreifen ist nicht mehr nötig, da mehrere Monate lang in einer Art „Tuning-Phase" die Blocking-Regeln festgelegt wurden. Wenn es doch einmal zu Problemen kommt, ist es trotzdem möglich, über das Webinterface von Arbor Ungewöhnliches – wie etwa zu hoher Datenverkehr aus bestimmten Ländern – zu identifizieren und per Mausklick ganz einfach zu blocken. Eine weitere **Erleichterung** sind die **verschiedenen Security-Levels** die mit den Farben Grün, Gelb und Rot markiert sind. Mit deren Hilfe können pauschal schärfere Regeln im Fall der Fälle geschaltet werden. „Das hat sich natürlich als sehr hilfreich erwiesen. Mit Level Gelb unterbinden wir beispielsweise unter anderem alle Suchmaschinen-Aktivitäten, um die Webserver zusätzlich zu entlasten, wenn das nötig sein sollte", erläutert Löhnert.

Die Vorteile des neuen Schutzes sind nachweislich spürbar: eine deutlich bessere Verfügbarkeit der Webserver und schnelle, einfache Reaktionen, falls doch mal Angriffe durchkommen, zeigen, wie gut das neue System das Hochschulnetz schützt. So konnte sich die seit April implementierte Lösung bei jüngsten DDoS-Attacken schon bewähren.

Über circular

Gegründet 1995, hat sich die circular Informationssysteme GmbH zu einem System- und Beratungshaus im Bereich IT-Infrastruktur entwickelt. Das umfangreiche Portfolio beinhaltet Lösungen rund um die Themen IT-Sicherheit, Data Center, Netzwerke und Communications. Die Dienstleistungskette reicht von der IT-Strategieberatung über die Projektplanung und -durchführung, die Lieferung von Hard- und Software, Systemintegration und Wartung bis hin zur Schulung. Neben dem Hauptsitz in Stuttgart unterhält das Unternehmen mit 70 Beschäftigten weitere Niederlassungen in München, Frankfurt, Berlin, Leipzig und Hamburg. Die IT-Spezialisten betreuen Kunden aus den Branchen Industrie, öffentliche Verwaltung, Service Provider, Finanzen, Gesundheitswesen sowie Forschung und Lehre.