Datenschutz

Zweifach gesichert

[31.08.2011] Um Anwendungen von Kunden wie den Stadtwerken Leipzig zu sichern, setzt IT-Dienstleister perdata auf ein zweistufiges Firewall-Cluster. Schadcode lässt sich so zuverlässig identifizieren. Zudem kann eine hohe Verfügbarkeit der Daten garantiert werden.

Die zur Stadtwerke Leipzig-Gruppe gehörende perdata Gesellschaft für Informationsverarbeitung unterstützt unter anderem kommunale Versorgungsfirmen in ganz Deutschland mit branchenspezifischen IT-Dienstleistungen. Um die zentralen Versorger- und Unternehmensanwendungen als Hosting-Lösungen anbieten zu können, betreibt der IT-Dienstleister zwei Rechenzentren in Leipzig. Die Verbindungen zu den Outsourcing-Kunden müssen zuverlässig abgesichert und hochverfügbar sein – hier setzt perdata an der Schnittstelle zwischen Rechenzentrum und Internet auf zweistufige und zertifizierte Firewalls.

#titel+Hohe Anforderungen an die Verfügbarkeit#titel-

Die Stadtwerke Leipzig als Muttergesellschaft sowie zahlreiche weitere kommunale Ver- und Entsorger wie die Stadtwerke Menden, Rosenheim oder Jena haben dem Dienstleister wichtige IT-Anwendungen anvertraut: beispielsweise Abrechnungs- und Handelssysteme für den Energievertrieb, Lösungen für die Logistik, die Buchhaltung oder das Controlling. Diese teils individuell angepassten Anwendungen laufen auf modernsten Servern, werden fortlaufend gepflegt und auf Wunsch auch redundant und somit hochverfügbar vorgehalten. Die Kunden greifen über verschlüsselte Internet-Verbindungen darauf zu. Wenn die Systeme dem Datenaustausch mit Dritten dienen, zum Beispiel Energieerzeugern, Dienstleistern oder dem Finanzamt, werden die Server in spezielle Sicherheitsbereiche gestellt – so genannte Demilitarisierte Zonen (DMZ). Die DMZ werden vom restlichen Netzwerk abgeschirmt, sodass externe Zugriffe von Dritten nur auf explizit freigeschaltete Systeme erfolgen können. Die Übergänge vom Rechenzentrum zum Internet sowie zu den DMZ werden mithilfe von Firewalls überwacht. An diese stellt perdata hohe Anforderungen: „Unsere Kunden aus der Versorgerbranche verlangen für zentrale Anwendungen Verfügbarkeiten von bis zu 99,9 Prozent. Diese Anforderungen können wir nur mit Firewalls erfüllen, die eine starke Sicherheitsleistung bieten und zuverlässig in ausfallsicheren Clustern arbeiten“, erläutert Holger Maschke, Prokurist und Bereichsleiter Systembetrieb bei perdata.
Für die Absicherung der kritischen Netzwerk-Übergänge wurde die Firewall GeNUGate von Anbieter GeNUA ausgewählt. Hierbei werden zwei verschiedene Firewalls – ein Application Level Gateway und ein Paketfilter – zu einem mehrstufigen System kombiniert. Daten aus dem Internet müssen beide Systeme passieren, um ins LAN des Rechenzentrums zu gelangen.

#titel+Firewall-Systeme ergänzen sich#titel-

Das Application Level Gateway ist zum Internet hin ausgerichtet. Es ist das aufwändigere der beiden Firewall-Systeme und überprüft den Inhalt des Datenstroms. Unerwünschter oder gefährlicher Code wird zuverlässig identifiziert und abgeblockt. Ist die Inhaltsprüfung bestanden, werden die Datenpakete zum zweiten Firewall-System, dem Paketfilter, geschickt. Dieser prüft formale Informationen wie Absender- und Empfängeradresse. Nur wenn die Verbindung gemäß den konfigurierten Regeln erlaubt ist, werden die Daten an den Empfänger im Rechenzentrum von perdata weitergeleitet. Die Kontrollmechanismen der beiden Firewalls arbeiten somit auf unterschiedlichen Ebenen und ergänzen sich. Ein weiterer Vorteil der

Zweistufigkeit: Die Demilitarisierten Zonen mit Servern, auf die externe Dritte zugreifen, können einfach zwischen den beiden Firewalls eingefügt werden. So sichert das Application Level Gateway in Richtung Internet, auf der anderen Seite separiert der Paketfilter die DMZ vom internen Netzwerk. „Durch die zweifache Prüfung mit Inhaltskontrolle bietet die Firewall starken Schutz. Auch wiederholte Penetrationstests konnten keine Schwachstellen aufdecken“, so Thomas Barth, Team-Leiter Netzwerk im Bereich Systembetrieb bei perdata.

#titel+Vom BSI geprüft#titel-

Zudem wurde GeNUGate vom Bundesamt für Sicherheit in der Informationstechnik (BSI) geprüft. Hier wurde als Maßstab der internationale Standard Common Criteria (CC) angelegt. Das Ergebnis ist ein Sicherheitszertifikat der höchsten Stufe EAL 4+. Da GeNUGate beim wichtigen Merkmal Selbstschutz noch höhere Anforderungen erfüllt, hat das BSI darüber hinaus den Zusatz Highly Resistant vergeben. GeNUGate ist die einzige Highly Resistant Firewall der Welt.
Die ausfallsichere Anbindung des Rechenzentrums an das Internet gewährleistet ein Firewall-Cluster: Am zentralen Übergang teilen sich zwei GeNUGates mittels Load Sharing die Arbeit. Sollte ein System ausfallen, übernimmt sofort der Partner dessen Aufgaben, sodass keine Verbindungen unterbrochen werden. Durch die Zusammenarbeit wird ein hoher Datendurchsatz sichergestellt, der bei steigenden Anforderungen durch die Einbindung zusätzlicher Firewalls in das Cluster gesteigert werden kann. Im Jahr 2000 hat perdata die erste GeNUGate-Firewall in Betrieb genommen, heute werden insgesamt acht dieser Systeme eingesetzt. „Damit erreichen wir das Sicherheitsniveau und die Verfügbarkeit, die wir garantieren müssen, um die hohen Anforderungen unserer Kunden aus der Versorgerbranche erfüllen zu können“, so Bereichsleiter Holger Maschke.

()

Stichwörter: IT-Sicherheit, perdata, GeNUA, Stadtwerke Leipzig