RZ-Dienstleister Grass-Merkur konsolidiert IT-Security-Infrastruktur

# Fortinet sichert IT für private Cloud-Services

Die Vereinfachung der Infrastruktur und die Reduzierung der Kosten durch geringeren Strom- und Betriebsaufwand - das waren die Ziele für Grass-Merkur, dem Hannoverschen Rechenzentrumsdienstleister, als es darum ging, die IT-Security zu konsolidieren. Zwei FortiGate-310b Appliances in einem hochverfügbaren Fortinet Cluster sorgen nun für eine deutlich reduzierte Komplexität und eine weitere Steigerung der Verfügbarkeit bei sinkenden Kosten.

Als Betreiber eines Rechenzentrums nach Bankenstandard vertrauen Kunden aus dem Finanzbereich ihre geschäftskritischen IT-Services den gesicherten Rechenzentrumsumgebungen der Grass-Merkur an. Durch das Outsourcing der IT-Services in die Private Cloud der Grass-Merkur sparen sie Kosten und erhalten eine garantierte Verfügbarkeit der Daten. Diese ausgelagerten, hochsensiblen Services erfordern ein Höchstmaß an baulicher und betrieblicher Sicherheit. Neben Sicherheitsschleusen und Videoüberwachung sorgt daher eine restriktive Zutrittskontrolle für maximale Sicherheit innerhalb der Gebäude. Von zentraler Bedeutung war jedoch die Absicherung der Daten gegen Angriffe aus dem Netz. Die verschiedenen internen Sicherheitszonen, in die das Hosting-Rechenzentrum aufgeteilt ist, wurden daher durch separate Firewall-Instanzen vom Backbone abgeschottet und durch acht dedizierte Firewall-Appliances geschützt.

**Jens Ahlbrand, Geschäftsführer bei Grass-Merkur: „Die Virtualisierungstechnik hat das Potenzial, viele physische Systeme kostengünstiger abzubilden. Dies bietet für uns den entscheidenden Vorteil."**

## Lange Backup-Zeiten

Die Appliances wurden den Anforderungen des Dienstleisters im Laufe der Zeit jedoch nicht mehr gerecht. Lange Backup-Zeiten, ein immer komplexeres Management sowie eine mühselige Fehlersuche und aufwändiger Betrieb führten dazu, dass sich Grass-Merkur nach einer neuen IT-Sicherheits-Option umsehen musste.

Bereits seit einem halben Jahr kooperierte der Dienstleister mit AirIT-Systems, einem Systemhaus mit Sicherheits-Fokus aus Langenhagen. Der Security-Spezialist sorgt für das tägliche Operating der Systeme und ist mit zertifizierten Systemingenieuren Fortinet Gold-Partner. Daher lag eine Konsolidierung der IT-Sicherheit mit Technologien von Fortinet auf der Hand. Überzeugend war jedoch in erster Linie das Angebot einer modernen Virtualisierungstechnik mit hoher Performance sowie sehr gute Erfahrung in der gemeinsamen Zusammenarbeit mit Fortinet.

## Verfügbarkeit gesteigert

„Die Virtualisierungstechnik hat das Potenzial, viele physische Systeme kostengünstiger abzubilden. Dies bietet für uns den entscheidenden Vorteil", erklärt Jens Ahlbrand, Geschäftsführer bei Grass-Merkur.
Die Herausforderung bestand darin, bei mindestens gleichbleibender Sicherheit, die Komplexität der IT-Security im Allgemeinen und insbesondere die Menge der eingesetzten Hardware in den internen Sicherheitszonen so weit wie möglich zu verringern. Davon versprach sich Grass-Merkur eine weitere Steigerung der Verfügbarkeit bei zeitgleich sinkendem Energieverbrauch und eine Reduzierung der „Point of Failures". „Unsere Cloud Service Level Agreements garantieren unseren Kunden eine Verfügbarkeit von bis zu 99,997 Prozent. Unsere alte Lösung leistete jedoch eine geringere Performance als die, die wir benötigen, um den Ansprüchen unserer Kunden gerecht zu werden. Mit dem neuen Cluster werden wir den hohen Standard eines Public Cloud-Services gerecht, den unsere Kunden erwarten. Die alten Appliances waren nur mit 10/100 Mbit/Sekunde Interfaces ausgestattet. So konnten wir eine Maximalgeschwindigkeit für große Datenmengen nicht erreichen.


**Geschäftssitz der Grass-Merkur GmbH & Co. KG in Hannover-Anderten.**

**Blick ins Grass-Merkur-Rechenzentrum (im Bild: Sun StorageTek L700e Tape Library, Fujitsu-Siemens Primecenter Racksysteme).**

Diese ist aber gerade bei Backup-Jobs unvermeidlich", so Ahlbrand. Zusammen mit AirITSystems migrierte Grass-Merkur die verschiedenen Sicherheitszonen des Rechenzentrums auf eine zentral positionierte Fortinet Hardware. Die ehemals acht teils redundanten Firewall-Cluster wurden auf einem hochverfügbaren Fortinet-HA-Cluster aus zwei FortiGate-310b abgebildet. Diese bilden nun wiederum acht virtuelle Firewalls ab. Der FortiGate Cluster stellt damit die zentrale Firewall-Instanz dar, mit dem mehrere tausend Anwender direkt oder indirekt verbunden sind. Sechs IT-Mitarbeiter sind für das Management der Appliances verantwortlich. Sie bilden das Kernteam des Security Operatings.

## Anforderungen erfüllt

Die Herausforderung lag bei der Implementierung des Fortinet Clusters in der Absicherung der Managed Services für die Cloud-Kunden. Die FortiGuard Antivirus sowie Intrusion und Detection Prevention (IDP) Services der FortiGates wurden diesen Anforderungen gerecht. Die neue VPN-Vernetzung ermöglicht es Cloud-Kunden nun sowohl eine IPSsec-VPN- als auch eine SSL-VPN-Verbindung zu nutzen. Als Knackpunkt erwiesen sich bei der Umstellung außerdem die Payment Card Industry Data Security Standards (PCI-DSS) Compliance-Forderung eines Kunden, der mit Kreditkarten-Daten operiert. „Die neuen Appliances erfüllen die PCI DSS Compliances absolut", versichert Ahlbrand.

Dank der leistungsstarken Virtualisierungstechnologie Inter-VDOM von Fortinet wurde die Umgebung mit den acht virtuellen Firewalls stark vereinfacht. „Das Abschalten der vielen dedizierten Firewalls reduziert die Komplexität und damit automatisch die Betriebskosten", so Ahlbrand. Die Inter-VDOM Links innerhalb des Clusters ersparen komplexe Routingkonfigurationen und ermöglichen zugleich ein homogenes Regelwerk über mehrere Firewallinstanzen hinweg. Mit den größeren Bandbreiten wird nun außerdem ein deutlich höherer Firewalldurchsatz erreicht. „Mit den enormen Performancewerten der 10/100/100Tx Interfaces der Fortinet Hardware steht uns eine zehnfach höhere Geschwindigkeit zur Verfügung. Damit verringerte sich vor allem das Zeitfenster für Backups deutlich", freut sich Ahlband. Insbesondere durch die Reduzierung der Strom- und Klimakosten um 75 Prozent hat sich der Fortinet Cluster ausgezahlt. Der Stromverbrauch der einzelnen Appliances wurde nicht verringert, jedoch die Anzahl von acht auf zwei reduziert. „Die geringere Anzahl an Appliances vereinfacht für uns auch das Monitoring, die Dokumentationsaufwendung und die System-Backups. Insgesamt ist der Betriebsaufwand damit um zirka. 20 Prozent gesunken. Dieses Ergebnis kann sich sehen lassen", so Ahlbrand. „Außerdem mussten wir vor der Umstellung auf teure Managementtools für die Appliances zurückgreifen. Dieses ist nun bei der Firewall nicht mehr notwendig."

## Ergebnis überzeugt

„Überzeugt haben uns bei Fortinet vor allem das Zeitmanagement und der Service. Die Migration auf Fortinet inklusive aller Netzarbeiten konnte an nur einem Wochenende durchgeführt werden - und das nahezu ohne Downtime! Außerdem spielte natürlich der Preis eine Rolle. Das gute Preis-Leistungsverhältnis bei Fortinet war mit ausschlaggebend, da für uns stand die Reduzierung der Betriebskosten ganz oben auf der Liste", resümiert Jens Ahlbrand.

www.fortinet.de
www.grass-merkur.de

Interview mit Thomas Koelzer, Vorstand secunet Security Networks AG:

# „IT-Sicherheit ist niemals eine Option“

**Chefbüro:** Das Bewusstsein der KMU beim Umgang mit IT-Sicherheit wurde lange Zeit als Kombination aus Ahnungslosigkeit und „Wird-schon-gutgehen“ beschrieben. Haben sich Denken und Verhalten verändert - angesichts der zunehmenden Angriffe auf Unternehmen und deren Daten?

Thomas Koelzer: Ein großflächiges Umdenken kann ich nicht feststellen. Die Beherrschung der aktuellen IT-Sicherheitstechnik ist für KMU eine große Herausforderung. Zudem werden die Anforderungen immer komplexer. Denn Sicherheitsrichtlinien, Firewall und Virenschutz allein reichen nicht mehr aus, um sich vor aktuellen Bedrohungen zu schützen. Software und Hardware sind zwar notwendige technische Hilfsmittel, aber letzten Endes ist die Strategie entscheidend. Und die muss jedes Unternehmen individuell aufstellen.

**Chefbüro:** Ist IT-Sicherheit Chefsache und wie viel muss der Chef von der Problematik verstehen?

Thomas Koelzer: Die Verantwortung für IT-Sicherheit wird meistens an die IT-Abteilung delegiert, aber IT-Sicherheit ist ein Thema des gesamten Unternehmens - und damit Chefsache. Technik und Bewusstsein müssen ineinander verzahnt sein, um den bestmöglichen Schutz der Daten zu gewährleisten. Auf die physikalische Sicherheit achten die meisten Unternehmen zum Beispiel sehr penibel. Sie haben Zutrittskontrollanlagen, teilen Ausweise an Besucher aus und überwachen ihr Firmengelände mit Kameras. Bei der

**Thomas Koelzer, Mitglied des Vorstands der secunet Security Networks AG, Essen: „Die größten Gefahren gehen für KMU nicht von Hackern aus, sondern ...**

Sicherheit ihrer IT tun sich viele häufig noch schwer. Das liegt daran, dass die Vorgänge innerhalb der IT abstrakter sind.
Um Entscheidungen zu treffen und Prozesse in Gang zu setzen, muss der Chef selbst kein IT-Experte sein, aber das Bewusstsein für das Thema mitbringen. Dann kann er seine IT-Abteilung oder, falls die eigenen Ressourcen zu knapp sind, einen externen Dienstleister beauftragen, den Status der IT-Sicherheit zu skizzieren. Auf dieser Basis kann er die notwendige Strategie und die erforderlichen Maßnahmen einleiten.

**Chefbüro:** Wo sehen Sie wesentliche Bedrohungsszenarien für KMU und wo entscheidende Schwachstellen einer Gefahrenabwehr?

Thomas Koelzer: Die größten Gefahren gehen für KMU nicht von Hackern aus, sondern liegen im Datenverlust, verursacht durch mangelhafte Policies, unachtsame Mitarbeiter und Mitarbeiter, die vorsätzlich handeln. Diese haben durch winzige USB-Sticks und schnelle Internetzugänge leichtes Spiel und können Konstruktionspläne, Arbeitsverträge und Kundendatenbanken aus dem Unternehmen schleusen. Aber es gibt technische Möglichkeiten, die diesen Datendiebstahl unterbinden oder zumindest aufzeichnen können. Angriffe von außen, wie sie aktuell für Schlagzeilen sorgen, werden häufig durch schlecht gewartete IT-Systeme begünstigt oder ermöglichen diese erst überhaupt.

**Chefbüro:** Kleinstunternehmen haben oft nur begrenzt Zeit, interne Mitarbeiter und Mittel für IT-Sicherheit. Wie können sie eine solche komplexe Aufgabenstellung gezielt angehen?

Thomas Koelzer: In erster Linie ist das eine Frage des Prozesses. Welche Daten habe ich, wie schützens-

**... liegen im Datenverlust, verursacht durch mangelhafte Policies, unachtsame Mitarbeiter ...**