

Sichere DNS und DHCP für die Reise in die digitale Welt.....

CASE STUDY

Systeme, Konzepte, Technologien – SCI Systems

Die Kernkompetenz der im westfälischen Kirchlingern gelegenen SCI Systems GmbH liegt in der Entwicklung, Planung und Umsetzung von innovativen Hard- und Software-Projekten. Den beiden Geschäftsführern Michael Kloehn und Sebastian Brandt ging es von Anfang an um beides: um individuelle und branchenübergreifende IT- und Telekommunikationslösungen; und zum anderen um intelligente First-Mover-Technologien, die das Unternehmen selbst in seinem IT-Team entwickelt. Dabei werden die Bereiche Storage, Sicherheit, IP-Communication, VoIP, Netzwerke und Managed Services, aber auch die Einbindung in bestehende ERP- und CRM-Lösungen abgedeckt.

Das gilt insbesondere für die inzwischen zur Realität gewordenen konvergenten Netze oder wenn es darum geht, verteilte Standorte in der Infrastruktur zusammen zu führen. Ziel ist denn auch nicht ‚nur‘ die entsprechenden Kommunikationstechnologien bereit zu stellen, sondern sie in ein komplettes Kommunikationskonzept einzubinden.

„Erfolgreiches unternehmerisches Handeln basiert auf lückenloser Information. Nur wenn Datenebene und Telekommunikation intelligent zusammen spielen, können auch die eigentlichen Kommunikationsmittel schneller, effektiver und wirtschaftlicher eingesetzt werden,“ umreißt Michael Kloehn das SCI-Konzept.

Hier setzen die entsprechenden Lösungen zum Archivieren und Speichern an. Das Datenvolumen in Unternehmen steigt weiter exponentiell an, und mit den wachsenden Anforderungen an ein intelligentes Datenmanagement sehen sich Firmen mit Sicherheitsrichtlinien und Compliance-Anforderungen konfrontiert.

„Hier schafft nur ein mehrstufiger Aufbau einer hochsicheren Umgebung Abhilfe,“ so Kloehn weiter. „IT-Sicherheit kann nur funktionieren, indem man eine ganzheitliche Strategie umsetzt, dazu gehören die Strukturen und Prozesse in einem Unternehmen und die technischen Systeme. Als Systemhaus haben wir ein besonderes Augenmerk auf die sensiblen Bereiche in der jeweiligen Branche.“

SCI Systems plant und implementiert auf dieser Basis eine für Branche und Unternehmen maßgeschneiderte Lösung, und unterstützt seine Kunden durch zusätzliche individuelle Beratungs- und Schulungsangebote.



“Wir können unsere Bedenken im Hinblick auf die externe DNS jetzt schlicht vergessen. Die Appliance läuft unterbrechungsfrei, sicher und zuverlässig, Änderungen in den Konfigurationen lassen sich problemlos umsetzen, und wir können effizienter für unsere Kunden tätig sein,“ ”

resümiert Michael Kloehn.

Zahlen und Fakten

- Kunde/Standort: SCI Systems GmbH, Im Obrock 37, D-32278 Kirchlingern
- Branche: IT-Systemhaus
- Mitarbeiter: > 15
- IT-Abteilung: 10 MA
- DNS/DHCP-Infrastruktur: 5 Windows-DNS/DHCP-Server
- Externe DNS: Adonis 750™ DNS/DHCP-Appliance zur Verwaltung externer DNS (Stand-Alone), 50 Kundendomains mit 500 DNS-Records
- Netzwerktopologie siehe Skizze

Vorteile und Nutzen:

- Hochsichere Appliance-Lösung
- Leicht zu implementieren
- Effiziente, einheitliche Verwaltung über zentrale Management-Konsole
- Stabile, zuverlässige, redundante Lösung für 24/7-Betrieb



Adonis™
DNS/DHCP Appliance



Kostenfreie Online-Demo unter:
www.bluecatnetworks.com/products/demorequest



BLUECAT NETWORKS™
The IPAM Intelligence Company

Keine Angst vor DNS und DHCP

Die SCI Systems hat an ihrem Standort in Kirchlingern insgesamt fünf Windows-basierte DNS/DHCP-Server im Einsatz. Zunehmendes Kopfzerbrechen bereitete dem IT-Team die DNS-Infrastruktur, die unter Windows-DNS betrieben wurde. Schwierigkeiten zeigten sich besonders im alltäglichen Betrieb, wenn Konfigurationen geändert oder angeglichen werden mussten. Auch auf den ersten Blick minimal erscheinende Ausfallzeiten von wenigen Minuten summierten sich bei vielfältigen Änderungen leicht auf.

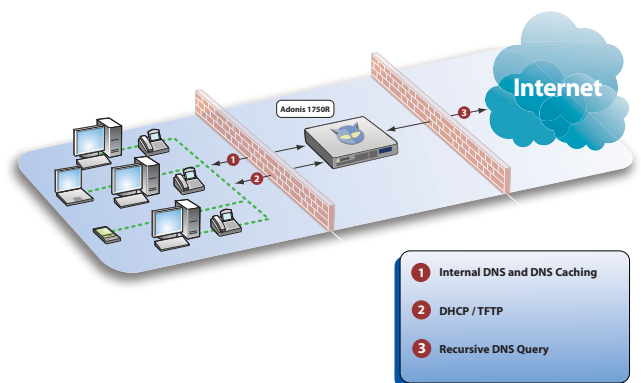
„Im Wesentlichen wollten wir drei Komponenten schnellstmöglich verändern und verbessern. Wir wollten eine sichere Lösung, die relativ leicht zu implementieren und zu betreiben sein sollte, und uns die Möglichkeit für ein zentralisiertes Management an die Hand geben würde; in unserem Fall für einen externen Stand-Alone DNS-Server, um die Domains unserer Kunden zu registrieren“, fasst Michael Kloehn das Anforderungsprofil zusammen.

Auch wenn DNS und DHCP quasi Synonyme für IP-Adressen sind, gehen ihre Aufgaben mittlerweile deutlich über das bloße Zuweisen einer Adresse beim Start des Computers hinaus. VoIP-Telefone holen sich per DHCP ihren Boot-Code vom Server, DNS-Server erfüllen über Reverse-Checks eine wichtige Aufgabe beim Kampf gegen Spam-Mails.

Das ist den SCI Administratoren natürlich bewusst, aber auch sie kämpften gelegentlich mit der immer komplexer werdenden Verwaltung der Dienste, zusätzlich sind die an Betriebssysteme gebundenen DNS/DHCP-Server Restriktionen unterworfen, auch wenn der eigentliche Funktionsumfang ausreichend ist. Hinzu kommt, dass ein DHCP-Server praktisch nie redundant ausgelegt ist, was in der Folge dann leicht zu Problemen führen kann. Fällt der Dienst aus, bleiben die neu zu startenden Arbeitsplätze ohne Verbindung zu den Ressourcen und Diensten im Netz, meistens sind auch VoIP-Telefone lahm gelegt.

Die Zeiten, in denen das Internet eine Insel des Reinen und Schönen war, für die DNS ursprünglich entwickelt wurde, sind lange vorbei. Sicherheit war nur rudimentär eingebaut, denn das Grundrauschen von Millionen von Spam-E-Mails, Attacken auf Webserver und zahllose Phishing- und Pharming-Versuche konnte und wollte man sich nicht vorstellen. Aktive Eingriffe in den DNS-Prozess wie Cache-Poisoning sind noch ungleich gefährlicher und können die Installation von Spyware oder Trojanern zur Folge haben, und auch Klick-Betrug ist keine Seltenheit. Gleiches gilt für Spoofing-Angriffe – sie benötigen keine Sicherheitslücken in der jeweiligen DNS-Software, sondern beuten die Art der Abfrage aus.

Hochverfügbar, ausfallsicher, auf einem hohen allgemeinen Sicherheitslevel sollte die neu zu installierende Lösung funktionieren. Bei SCI kam noch dazu, dass der öffentliche DNS-Server möglichst leicht zu implementieren und zu managen sein sollte.



Sicheres DNS-Management

„Wir brauchten einen SCI-eigenen DNS-Server zur Registrierung unserer Kundendomains,“ erklärt Michael Kloehn. „Neben einem möglichst geringen Administrationsaufwand benötigten wir einen deutlich höheren Sicherheitslevel und ein besonders stabil laufendes, redundantes System. Wir waren mit BlueCat Networks bisher noch nicht vertraut und sind erst durch einen Bericht in den Medien aufmerksam geworden, haben aber dann zeitnah mit der Recherche begonnen. Schon in dieser frühen Phase war der Support für uns da und zeichnete sich durch Kompetenz und Verständnis für unser Anforderungsprofil im Hinblick auf die gewünschte DNS-Konfiguration aus.“

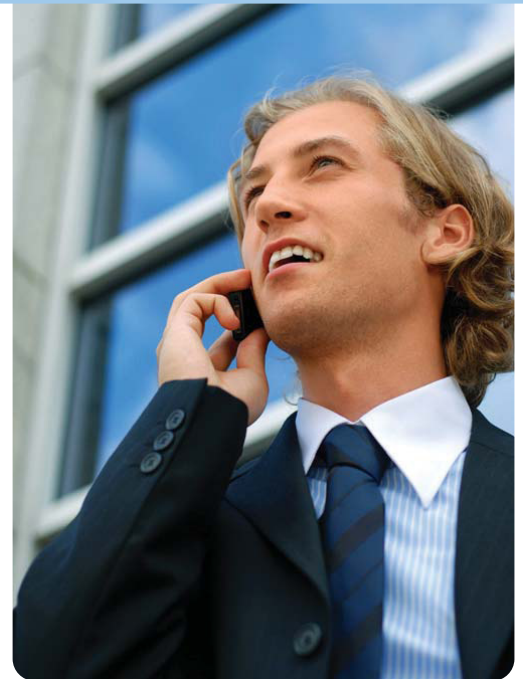
Als sich dann im Unternehmen die Möglichkeit bot, das Produkt zu evaluieren, entschied man sich zügig für eine Implementierung der Adonis 750 Appliance als externe Stand-Alone DNS-Variante. Bevor man auf die Adonis-Appliances von BlueCat Networks stieß, nahm man auch die zur Verfügung stehenden Windows DNS/DHCP-Lösungen, ISC DHCP und Sun DNS genau unter die Lupe.

„Das Konzept einer Appliance-Lösung für DNS hat uns überzeugt, denn auf diese Weise können wir unsere Kundendomains sicher registrieren und zentral verwalten; auch Updates und Konfigurationsänderungen sind völlig unproblematisch. Eines der wichtigsten Features der Adonis-Appliance ist die Fail-Over-Funktion, um einen 365/24/7-Betrieb garantieren zu können,“ so Kloehn.

BlueCat Networks verfolgt bei DNS, wie beim übergreifenden Management von IP-Adress-Daten ein eigenes Konzept: der DNS-Server wird als Appliance geliefert, fertig installiert, mit einem gehärteten und hochsicheren Betriebssystem als Basis. Die DNS/DHCP- und so genannten ‚IPAM‘-Appliances skalieren dabei von ein paar Dutzend Anwendern bis hin zu weltweit verteilten Netzwerken mit vielen hunderttausend Clients.

Die zugrunde liegende Management-Plattform wurde unter Praxis Gesichtspunkten entwickelt, und ist von eigentlichen Service-Layer getrennt, so dass im Falle eines Falles auch beide unabhängig voneinander funktionieren. Das vereinfacht auch die Verwaltung des Service, während die strenge Verschlüsselung zwischen gegebenenfalls mehreren Appliances für einen erhöhten Sicherheitslevel sorgt.

„Die Teststellung bewährte sich sehr schnell im Real-World-Einsatz. Auch wenn wir zunächst einige Einstellungen als gewöhnungsbedürftig empfanden, lief die Box ausgesprochen sicher, stabil und zuverlässig. Deshalb entschieden wir uns nach der Testphase zügig für den Einsatz in der endgültigen Konfiguration hinter den beiden Firewalls. Inzwischen verwalten wir 50 Kundendomains und 500 DNS-Records mit der Adonis-Appliance,“ ergänz Michael Kloehn.



Fazit

Michael Kloehn zieht ein positives Fazit: „Wir können jetzt schon sagen, dass sich unsere Erwartungen positiv bestätigt haben und sich die Adonis-Appliance bewährt. Wir haben derzeit eine Maschine in der beschriebenen Konfiguration im Einsatz, und erwägen den Einsatz einer weiteren, um eine noch bessere Fehlertoleranz und komplette Redundanz zu erzielen. Die DNS-Administration für unsere Kunden hat sich ganz erheblich vereinfacht, und wir sparen hier viel Zeit und Ressourcen, die wir anderweitig einsetzen können.“

BlueCat Networks Inc. Telefon: +49 (0) 6227 381-115
 sblasius@bluecatnetworks.com
 www.bluecatnetworks.com

