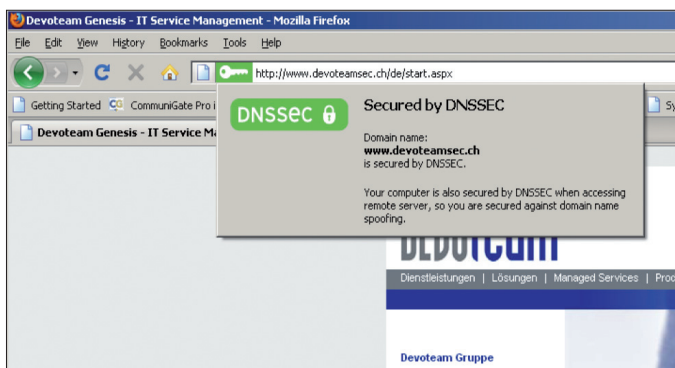


DNSSEC – Für ein sicheres Internet

Jeder von uns kennt und nutzt DNS, das Domain Name System. Weniger bekannt hingegen ist die latente Gefahr, die DNS unterliegt. In den frühen Tagen des Internets spielten für grundlegende Protokolle und Dienste Sicherheitsaspekte kaum eine Rolle. Ebenso sind im einfach aufgebauten DNS keinerlei Techniken gegen Missbrauch implementiert. Getrieben vom Bekanntwerden der Kaminsky-Attacke und US-Regulatorien hat das Thema DNSSEC während der letzten Monate an Bedeutung gewonnen. DNSSEC, die Abkürzung für DNS Security Extensions, soll nun dem Namensdienst die bemängelte Sicherheit hinzufügen.



DNSSEC ist eine Erweiterung von DNS, welche die Authentizität und Integrität von DNS-Antworten gewährleistet. Es wird in der Fachwelt als die Lösung für das Cache-Poisoning-Problem gehandelt. DNSSEC stellt die einzige verfügbare Möglichkeit dar, die Manipulation von DNS-Daten auf dem Transportweg zu verhindern. Vereinfacht gesagt: DNSSEC ist eine Art Versicherung, die dem Internetnutzer garantiert, dass nur diejenige Webseite angezeigt wird, die er aufrufen will. Bei DNSSEC werden keine Informationen verschlüsselt. Alle Daten bleiben wie beim bestehenden DNS öffentlich zugänglich.

Wieso braucht man überhaupt DNSSEC?

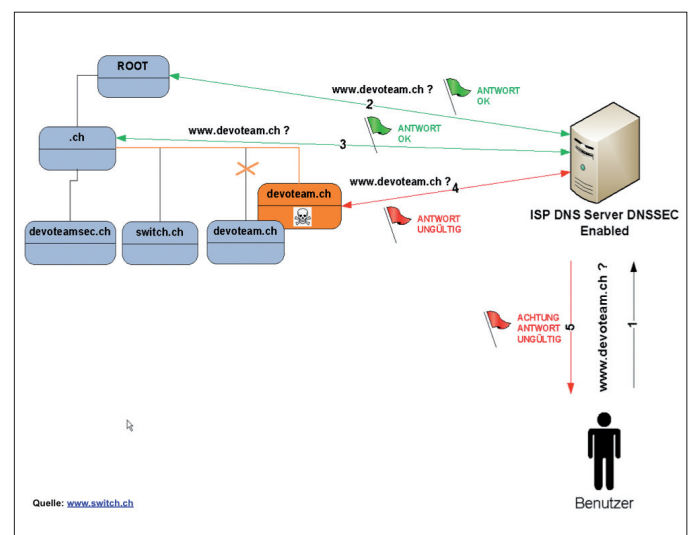
Der aufmerksame Leser hat sicher erkannt, dass im Internet Browser schon eine Technologie integriert ist, welche dem User die «richtige» Webseite garantieren soll. Solche Webseiten sind meist mit SSL (Secure Sockets Layer) verschlüsselt. DNSSEC wurde nicht entworfen, um die SSL-Verschlüsselung abzulösen. Im Gegenteil, DNSSEC soll SSL

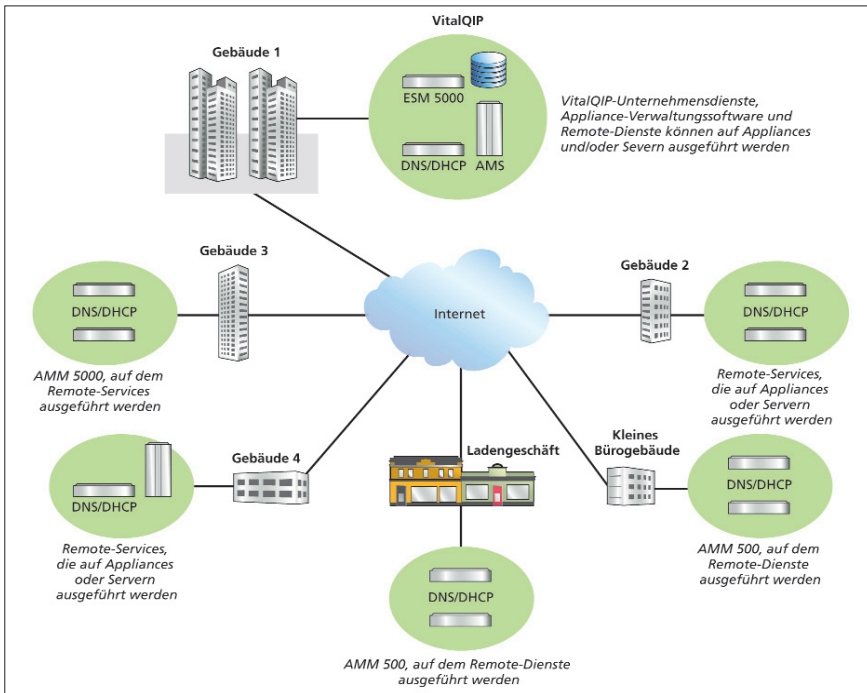
ergänzen und verhindern, dass man nicht schon auf einem falschen Server landet, bevor die Verbindung durch SSL gesichert wurde. Falls es einem Angreifer gelingt, zum Beispiel falsche Daten in den Server Ihres Providers einzuschleusen (Cache Poisoning), würden Sie beim Aufruf von z.B. www.devoteam.ch auf einer anderen Webseite landen. Stellen Sie sich besser nicht vor, was passieren könnte, wenn es sich bei der gefälschten Webseite um die Ihrer Bank handelt.

Obwohl das grundsätzliche Design von DNSSEC bereits vor mehreren Jahren entwickelt wurde, gab es über lange Zeit aufgrund des hohen Aufwandes und dem Fehlen entsprechender Hilfsmittel kaum Interesse an einer praktischen Umsetzung im Internet oder in Firmennetzwerken. Ausgelöst durch die Kaminsky-Attacke und eine Initiative der US-Regierung ist jedoch mittlerweile sehr viel Bewegung in die Einführung von DNSSEC gekommen. Seit dem 1. Februar 2010 ist es bereits möglich, bei Switch signierte .ch und .li Domänen entsprechend zu registrieren. Weitere Toplevel-Domains sind bereits mit Hilfe von DNSSEC signiert, zahlreiche weitere werden während der nächsten ein bis zwei Jahre folgen. Zahlreiche Hersteller von DNS-Lösungen liefern mittlerweile erweiterte Funktionalität, um den Betrieb von DNSSEC zu erleichtern. Auch die Referenz-Implementierung ISC-Bind wird stetig mit dieser Zielsetzung weiterentwickelt.

Herausforderung IP-Adressen-, DNS- und DHCP Management

In den letzten Jahren hat die Komplexität der IT-Infrastruktur, und somit die Wichtigkeit von IP-, DNS- und DHCP-Services, stark zugenommen.





Beispiel für eine VitalQIP Appliance-Konfiguration

Doch die Herausforderung, sprich die Schwierigkeit diese Services richtig zu verwalten, besteht nach wie vor. Innerhalb der IT gehören DNS- und DHCP-Services zu den businesskritischen Faktoren. Das Management von IP-Services ist jedoch ein wenig ins Abseits geraten, weil die Businessrelevanz nicht unmittelbar erkennbar oder belegbar ist. Aber was passiert, wenn zum Beispiel der DNS-Service ausfällt, inkorrekte oder keine IP-Adressen vergeben werden? Es fallen wichtige Applikationen aus! Zuverlässige IP-Dienste sind nach wie vor für die Verfügbarkeit und die Endnutzerleistungen und somit auch für Ihren Geschäftserfolg von grosser Bedeutung. Um die Qualität von IP-Services zu garantieren, ist es deshalb heute unabdingbar, über ein zuverlässiges, sicheres und kostengünstiges IP Adressen Management zu verfügen.

Anforderungen an ein modernes IPAM-System

- zentrales IP-Management
- Mandantenfähigkeit, hierarische Administration
- Redundanz der DNS/DHCP Server (High Availability)
- mögliche Anbindung an andere Systeme
- Einbindung vorhandener DNS/DHCP Server
- dedizierte DNS/DHCP Appliances

Mit den Lösungen Alcatel-Lucent VitalQIP und Infoblox bietet Devoteam Genesis zwei moderne und bewährte Verwaltungslösungen an, welche je nach Umgebung und Bedürfnissen zum Einsatz kommen. Mit diesen Lösungen werden Dienste für die Adressverwaltung über IPv4- und IPv6-Netzwerke bis hin zu den Namensdiensten wie DNS und DNSSEC voll automatisiert. Zusammen mit

hochverfügbaren DNS/DHCP Appliances decken diese Lösungen die Anforderungen an ein modernes IPAM-System vollständig ab.

Zusammenfassung

In naher Zukunft wird kein DNS-Administrator darum herumkommen, sich intensiv mit der Thematik DNSSEC auseinanderzusetzen, insbesondere wenn es um den Betrieb des Internet-DNS geht. Was bedeutet das konkret für Ihre DNS-Server-Umgebung? Devoteam Genesis unterstützt Sie bei allen Fragen rund um DNSSEC und zeigt Ihnen auf, welche Möglichkeiten unsere Lösungen für eine automatisierte Bereitstellung aller IP-Dienste inkl. DNSSEC bieten. Als zertifizierter Alcatel-Lucent- und Infoblox-Premier-Partner bieten wir seit 1996 erfolgreich IP-Management-Lösungen an. Unsere

langjährige Erfahrung in mehr als 100 erfolgreichen, zum Teil weltweiten Projekten, sind unser Erfolgsausweis für Sie.



Infoblox Appliance 1550

DEVOTEAM GENESIS

Planen Realisieren Betreiben

Lösungen für IT Service Management, IT Security Management, IP Management

Unsere Erfolgsgarantie

Seit 1996 Komplettlösungen aus einer Hand, durchgängige Kompetenz, internationale Ressourcen, Spezialisten-Know-how, Expertise und Erfolg in grossen IT-Umgebungen

Kontakt

Ostermundigen / Zürich / Carouge
 Tel. 031 560 35 35 Fax 031 560 35 45
 Tel. 044 455 60 81 Fax 044 455 60 85
 Tel. 022 732 16 27 Fax 022 732 16 28
 info@devoteam.ch

www.devoteam.ch