

Sonderdruck für SHD System-Haus-Dresden

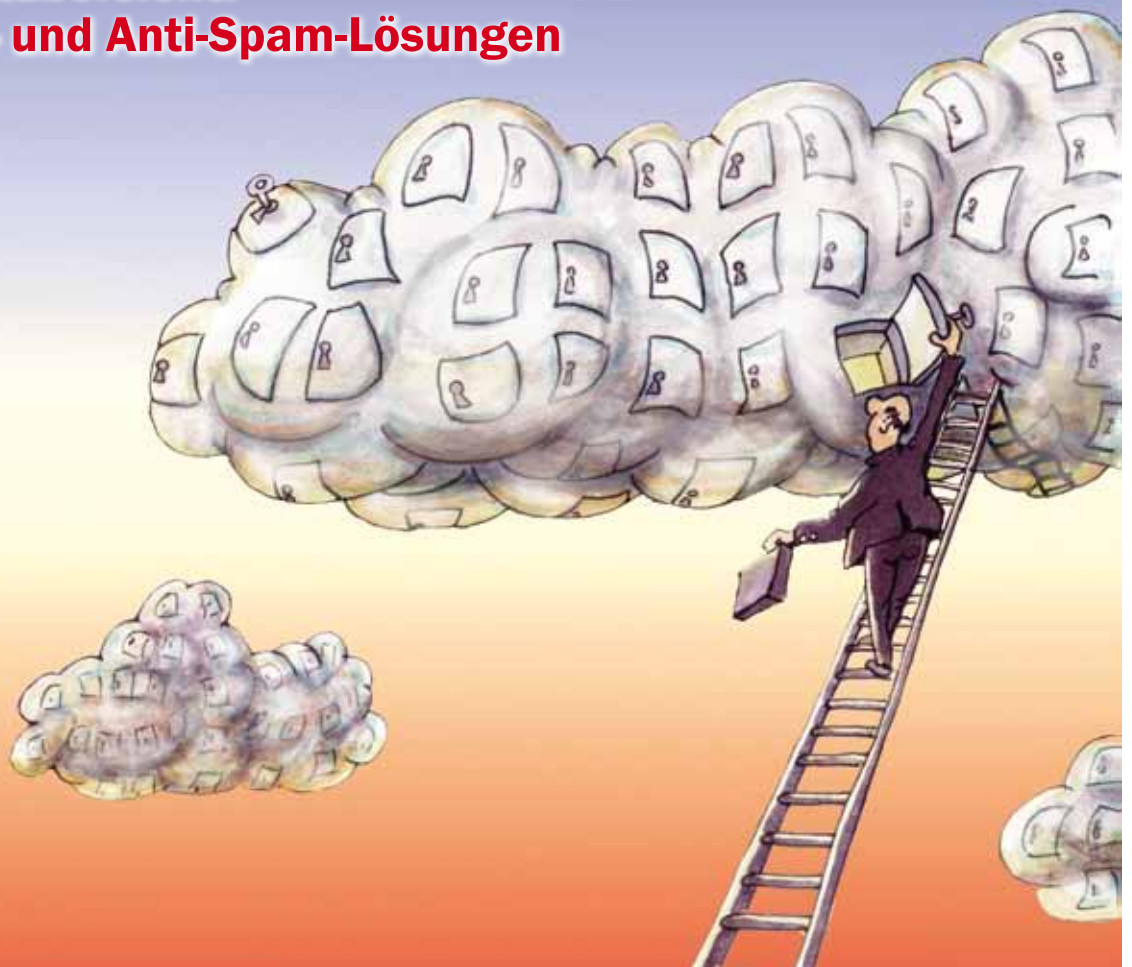
Security und Remote Access

Identity- und Access-Management in der Cloud

Private Smartphones und Tablets im Unternehmen

Dynamische Desktops

**Mit Marktübersicht:
Antivirus- und Anti-Spam-Lösungen**



Der Nutzen einer Netzwerkdokumentation

Der Plan vom Netz

Eine Netzwerkdokumentation hat nicht nur bei einem Störfall einen unschätzbaren Wert. Abhängig von der Intelligenz der verwendeten Werkzeuge ist bisweilen jedoch ein immenser Aufwand nötig, um den aktuellen Stand darzustellen. Eine Lösung von SHD soll die Arbeit erheblich erleichtern.

Es ist allgemein anerkannt, dass zum sicheren Betrieb einer komplexen Infrastruktur eine exakte Dokumentation gehört. In diese Richtung zielen auch die Vorschriften gemäß Sarbanes Oxley Act oder „Euro-SOX“, Basel II und III sowie die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS). Umweltereignisse – zum Beispiel die Überschwemmungen durch die Elbe im Jahr 2002 oder die Katastrophe dieses Jahres in Japan – haben die Sicht auf die Verfügbarkeit der IT-Infrastruktur direkt verändert. Spätestens Zertifizierungen nach ISO 2700x oder ISO 20000 fordern eine aktuelle Dokumentation der passiven und aktiven Netzwerkinfrastruktur.

Dennoch ist der laufende Betrieb einer IT-Infrastruktur mit Aufgaben und Prioritäten für das Personal in der Weise und dem Maß verbunden, dass vielfach für das Thema Netzwerkdokumentation nicht mehr ausreichend Ressourcen verfügbar sind. Die Praxis umschreibt mit dem Begriff „historisch gewachsen“ einen Zustand des IT-Netzwerks, der meist einer dringenden Veränderung, aber mindestens einer exakten Dokumentation bedarf. Diese Situation wird zusätzlich dadurch verschärft, dass selten der tat-

sächliche Nutzen einer Netzwerkdokumentation klar ist und der Pflegeaufwand überschätzt wird.

Auf dem Markt sind drei verschiedene Lösungsansätze für das Problemfeld Netzwerkdokumentation erkennbar: Es gibt die klassischen Kabel-Management-Systeme,

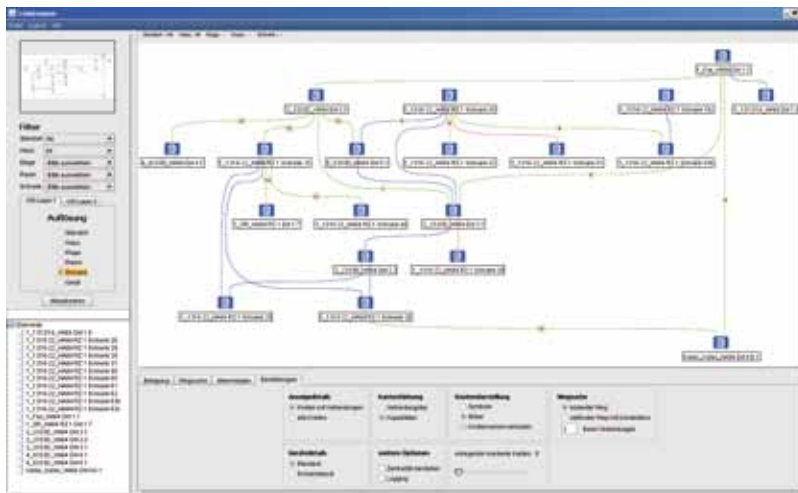


Bild 1. Netzwerkschränke mit den freien Verbindungen untereinander.

die eine datenbankgestützte, fasergenaue Beschreibung der Infrastruktur und der erforderlichen Veränderungen im Betrieb ermöglichen. Der Vorteil dieser Systeme besteht unter anderem in einer exakten Dokumentation aller Veränderungen der passiven Infrastruktur des Netzwerks. Ein Nachteil dieser Lösungskonzepte ist der enorme Pflegeaufwand, da Automatisierungen in der Datenerfassung kaum möglich sind. Des Weiteren ist der Nutzen für die tägliche Arbeit im IT-Betrieb eher gering.

Dem entgegen steht eine Tendenz zur automatisierten Datenerfassung mit unterschiedlichen Tools, die SNMP-, Netbios- oder WMI-Daten erfassen und auswerten. Der Vorteil dieses Ansatzes ist sicher, dass die entstehenden Dokumentationen automatisch erstellt und fortgeschrieben werden können. Dieser Ansatz hat jedoch den Nachteil, dass in der physischen Ebene nur aktive Komponenten erfasst werden und die gesamte Verkabelung außen vor bleibt. Damit fehlen gerade zur Analyse von Netzwerkproblemen oder Sicherheitsvorfällen die notwendigen Daten.

Als gelebter Mittelweg für kleinere und mittlere Unternehmen lässt sich die Netzwerkdokumentation als Sammlung der erforderlichen Informationen mit unterschiedlichen Strukturen und Inhalten verstehen, die im Rahmen eines Dokumentationsprojekts sukzessive zusammengetragen und gepflegt werden. Vorteile dieses Herangehens sind sicher, dass eine übersicht-

liche, strukturierte Dokumentation entsteht und der Anwender selbst über die Detailliertheit seiner Dokumentation entscheidet. Nachteilig ist auch in diesem Fall, dass die Pflege überwiegend manuell erfolgt. Eine Überprüfung der Aktualität ist nur sehr schwer möglich.

Die von SHD (System-Haus-Dresden) entwickelte Lösung namens „SM-Docu“ zielt darauf, eine praktikable Integration dieser aufgeführten An-

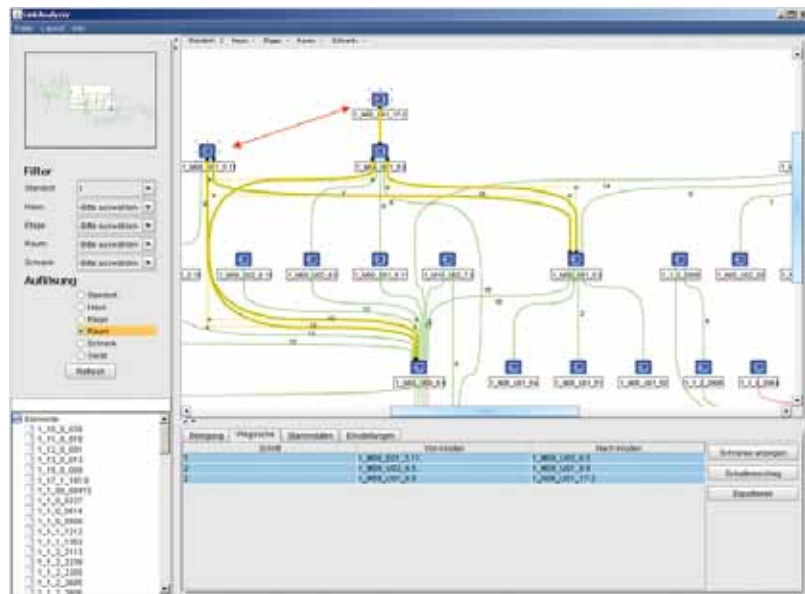
sätze zu erreichen. Dabei gab es wichtige Vorgaben:

- Die datenbankgestützte Lösung ist der richtige Weg, um wachsende Strukturen abbilden und die Daten für ein Team im gesamten Netzwerk bereitstellen und im Team gemeinsam bearbeiten zu können;
- die Darstellung der Informationen zur physikalischen Ebene mit einer grafischen Oberfläche ist nutzerfreundlich, erleichtert die Arbeit und reduziert die Fehlerwahrscheinlichkeit bei der Datenerfassung;

- die Verbindung der Daten der physischen Ebene mit den Daten der höheren Netzwerkschichten (etwa den Port-Informationen der Switches) schafft Mehrwerte für die Dokumentation;
- die Nutzung der dokumentierten Informationen, um beispielsweise redundante Wege zu finden, Schaltvorschläge zu ermitteln und beliebige Topologiedarstellungen zu erzeugen; und
- diese Daten einer übergeordneten Konfigurationsdatenbank (CMDB/CMS gemäß ITIL) zur Verfügung zu stellen.

Dabei ist laut SHD berücksichtigt, dass viele Daten der Netzwerkdokumentation relativ statischer Natur sind und der Erfassungs- und Pflegeaufwand damit relativ gering bleibt – oder sogar in erster Näherung einmalig ist. Dies betrifft zum Beispiel die territorialen Daten (Standort, Häuser, Etagen, Räume, Primär- Sekundär- und Tertiärverkabelung). Wesentlich aufwändiger gestaltet sich die Erfassung und Pflege der Daten der aktiven und passiven Geräte in den Datenschränken und der Geräte in den Arbeitsräumen (Endgeräte). Die aktiven Geräte (Switches, Server, Storage-Systeme, PCs der Anwender etc.) lassen sich mit Discovery Tools erfassen und auswerten. Diese Auswertungen können jedoch immer nur Informationen über die ausgewertete Hardware und die logischen Zusammenhänge darstellen. Soll eine umfassende Dokumentation über alle Netzwerkschichten – also auch die physische Schicht – entstehen, sind zwei Informationsarten zwingend per Hand zu pflegen: die Position der Geräte in einem Datenschrank und der einzelne Patch.

Letztere Information ist die, die sich im Rahmen eine Netzwerkdokumentation erfahrungsgemäß am häufigsten ändert. Alle bisher bekannten Lösungen zur Automatisierung des Patch-Managements sind mit erheblichen Investitionen in zusätzliche Hard- und Software (Patch-Panel, Scanner, Software) verbunden, die sich erst in größeren Unternehmen in überschaubaren Zeiträumen bezahlt machen. Die Minimierung dieser Arbeitsaufwendungen in der täglichen Arbeit war ein Ziel der Entwicklung der GUI von SM-Docu. Dazu gibt es zwei grafisch orientierte Menüs, die per



Verfolgung von Umzügen einzelner PCs unterstützen. Auf der Basis dieser Datenverknüpfung kann der Administrator nun auch automatisch ermitteln, wie aktuell die Netzwerkdokumentation bezogen auf die manuelle Erfassung der Verkabelungsdaten ist. Durch Differenzlisten lässt sich aufdecken, welche Ports beschaltet, aber nicht dokumentiert sind. Über die Historie lässt sich auch schnell entscheiden, ob ein Port noch genutzt wird oder ob er „entpatch“ werden kann.

Eine Dokumentation, die nicht zum Selbstzweck erstellt wird und die daher viele IT-Mitarbeiter nutzen, benötigt einen Client-losen Zugriff. Durch eine nur lesende Web-Schnittstelle ist dies in SM-Docu gewährleistet. Während es zunächst nur um die Realisierung eines Browser-basierenden Zugriffs auf die Daten ging, rückte immer mehr der Nutzen für die tägliche Anwendung in den Vordergrund.

Das Modul Link Analyzer unterstützt eine automatische Visualisierung von Netzwerkstrukturen und ermöglicht so eine grafische Sicht auf die strukturiert vorliegenden Daten. Diese Java-Komponente analysiert die in der Datenbank dokumentierten Verbindungen im Bereich der Primär- und Sekundärverkabelung und zeigt entsprechend Filtereinstellungen Netz-Knoten (Häuser, Technikräume, Schränke, Geräte) und die (freien) Verbindungen (Bild 1) zwischen diesen Knoten an. Mit diesen Informationen sind die Fragen nach der Wegesuche, der automatischen Erstellung von Schaltvorschlägen und der Export in eine Datei naheliegend. In einem

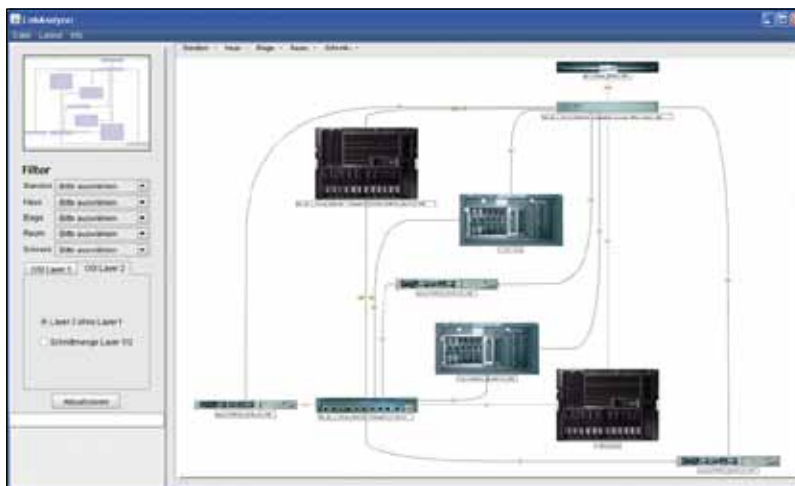


Bild 3.
Darstellung
der Layer-
2-Topologie.

gut durchdachten Netzwerkdesign findet der Link Analyzer dann auch redundante Wege (Bild 2).

Diese Funktionalität des Link Analyzers basiert zunächst nur auf einer Betrachtung der Layer-1-Daten. Aufgrund der zuvor dargestellten Verknüpfungsmöglichkeiten mit Layer-2/3 Daten aus dem Netzwerk-Management kann eine Analyse der SM-Docu-Datenbank so auch Layer-2-Topologien erzeugen. Bild 3 zeigt ein solches Beispiel und stellt dar, wie eine automatisch erstellte Layer-2-Topologie aussehen kann.

Dass an dieser Stelle der Einwand kommt, dass dies die Management-Systeme schon lange können und wozu man also noch eine Datenbank benötige, die eine solche Visualisierung anbietet, ist nur zu verständlich und auch berechtigt. Was jedoch kein Netzwerk-Management-System dieser IT-Welt kann, ist die Visualisierung der Verknüpfung dieser Layer-1-Dokumentation

mit der Layer-2-Topologie, und zwar ohne den manuellen Aufwand einer Visio Zeichnung. Außerdem ist das Ganze jederzeit automatisch aktualisierbar.

Damit ist der manuelle Erfassungs- und Pflegeaufwand der Datenbank sicher durch den Nutzen relativiert, jederzeit vom Prüfer/Auditor geforderte aktuelle Netzwerktopologieübersichten vorweisen zu können. Da Netzwerke keine statischen Objekte sind, ist der Aktualisierungsaufwand jeder manuell erstellten Dokumentation erheblich. Damit gehören nicht nur Excel-Listen für die Netzwerkdokumentation der Vergangenheit an, sondern auch die Visio-Zeichnungen innerhalb von Systemdokumentationen. Diese lassen sich aus dem Link Analyzer erzeugen und als Grafik speichern. Der Link Analyzer als Bestandteil der Lösung ist ein Instrument, diesen Aktualisierungsaufwand zu vermeiden und stattdessen für die Pflege der Detaildaten in der Datenbank einzusetzen. Im Ergebnis sind auf der Grundlage der Menge der Detaildaten alle für einen sicheren Betrieb und die erforderliche Verfügbarkeit der Netzwerkinfrastruktur erforderliche Sichten der Dokumentation erzeugbar.

Dr. Detlef Geisler, Robert Sieber/jos



Bild 4.
Layer-1-
und Layer-
2-Topologie
in einer ge-
meinsamen
Darstellung.

- SHD System-Haus-Dresden GmbH
www.shd-online.de
- Dr. Detlef Geisler
Geschäftsstellenleiter Hamburg
Tel. 030/53330-120
E-Mail detlef.geisler@shd-online.de
- Robert Sieber
Teamleiter Produktmanagement
Tel. 0351/4232-173
E-Mail robert.sieber@shd-online.de