

13.07.09

Von: Thomas Brosch

Wide Area Network & WAN Security: die IT vom Aufbau bis zur Echtzeit-Überwachung



Gefragt sind Sicherheit, Zuverlässigkeit und Kosteneffizienz. Viele Aspekte gilt es zu realisieren, wenn es um die Vernetzung von Unternehmensstandorten geht.

Die Bereitstellung des eigentlichen Netzwerks inklusive Bandbreitenoptimierung, globale Zugriffsmöglichkeiten, der Schutz vor Angriffen und Datensicherung – es bedarf innovativer Technologien und kreativer, individueller Lösungen, um den Anforderungen eines Unternehmens bei der Kommunikation mit seinen weltweiten Niederlassungen gerecht zu werden.

High Security Verbindungen bis in Krisenregionen

Der Aufbau eines Netzes mit stabilen Verbindungen auch bis an exotische Standorte kann durch differenziert eingesetzte Techniken ermöglicht werden, letztlich ohne, dass das Unternehmen selbst davon viel mitbekommt. Ob der Datenaustausch mit einer Niederlassung per Satellit oder wenn nötig sogar über Funkstrecken erfolgt, ist für den Betrieb zweitrangig und eben die Aufgabe des Dienstleisters.

Corporate Networks auf MPLS- und/oder IPSEC-VPN-Basis, Backups über Funk oder ISDN, UMTS Zugänge für Remote-Clients – immer in Kombination mit entsprechenden Security-Lösungen. Mit Hilfe hochwertiger Firewall-Hardware und einem profunden Sicherheitskonzept, das auch Verschlüsselungen, Antivirus und Antispam beinhaltet, lässt sich das Weitverkehrsnetz auch über viele Länder und verschiedene Carrier hinweg gegen unberechtigte Zugriffe von außen sichern. Der Markt bietet auch BSI-zertifizierte Hochsicherheitssysteme an, die über eine doppelte Verschlüsselung die sichere Übertragung als streng geheim klassifizierter Dokumente erlaubt.

WAN Optimierung und stabile IT-basierte Geschäftsprozesse

Auch für den Betrieb bestehender Unternehmensnetzwerke sichert ein Fein-Tuning des

Netzwerkes den effizienten und zuverlässigen Betrieb. Eine Bandbreitenoptimierung ermöglicht auch über Schmalbandleitungen einen hohen Durchsatz an Informationen. Tritt der Datenstrom aus einem Breitbandbereich (LAN) in ein Netzwerk mit geringerer Bandbreite ein (WAN), kommen Kompressions- und Musterersatzverfahren zum Zuge, die den gleichen Informationsinhalt mit einem minimierten Datenaustausch bewerkstelligen. Übertragungen unnötiger Broadcasts werden gefiltert, sich ständig wiederholende Sequenzen werden gemarkert und nur einmal über die Leitung geschickt. In diesem Fall ist die entsprechende Hardware, etwa ein Router mit Kompressionsmodul, an beiden Enden der Leitung vonnöten.

Eine weitere Entlastung für die Leitung und ein zusätzliches Feature für den stabilen WAN-Betrieb sind Proxy- und Cachingsservices, die auch bei kurzzeitigen Aussetzern der Leitung die Verbindung aufrecht erhalten und so das Fortsetzen einer begonnenen Session ermöglichen.

Um auch bei Spitzenauslastungen die Funktion für den Geschäftsbetrieb wichtiger Applikationen und Protokolle wie Mails oder Datenbankabfragen zu gewährleisten, können intelligente Systeme zur Datenpriorisierung den Datenverkehr in Priorisierungsklassen ordnen und im Betrieb verwalten.

Data Protect & Security: inkrementelle Backups und Storage

Von Vorteil für die gesamte Unternehmenskommunikation bis hin zum mobilen User ein Stockwerk tiefer oder im Outback sind Komplettlösungen, die nach dem Baukastenprinzip die aus der Bedarfsanalyse erstellten individuellen Anforderungen spezifisch umsetzen.

Ein weiterer wesentlicher Teil einer soliden IT-Infrastruktur ist die Erstellung von Backups. Replizierte Daten werden komprimiert und verschlüsselt über das WAN an einen Auslagerungsstandort wie ein eigenes oder ein externes gehostetes Ersatz-Rechenzentrum übertragen, im besten Falle sind auch zum Beispiel MS Exchange- oder Domino-Daten über Applikation-Plug-Ins bitweise und im besten Falle inkrementell direkt von Außenstellen-Arbeitsstationen zentral gesichert.

Gefährdungen im Netzwerk durch KI frühzeitig erkennen

Von der Nachauswertung zur handlungsfähigen Vorhersage – zwar lassen sich alle Netzwerk-Aktivitäten eines WANs in Echtzeit überwachen und eine Reaktion auf akute Ereignisse ist unmittelbar möglich. Doch ist es schon jetzt schwierig, teuer und zeitaufwändig, die Daten zu korrelieren und auszuwerten. Die Vision einer Forschungsgruppe ist es, mittels künstlicher Intelligenz ein System zu schaffen, das ein proaktives Agieren durch die frühzeitige Erkennung von Angriffen ermöglicht.

Um auf dem Gebiet der Internet-Security neue Technologien und Möglichkeiten zu entwickeln, wurde das Forschungsprojekt FIDeS ins Leben gerufen. Das Frühwarn- und Intrusion Detection System soll auf der Basis kombinierter Methoden der Künstlichen Intelligenz die Auswertung und Analyse von Anomalien im Datenverkehr ermöglichen. Statistische Langzeitdaten und Echtzeitlogs aus dem Datenstrom sollen verglichen und beurteilt werden, so dass Angriffsmuster schon im Vorfeld erkannt und Maßnahmen ergriffen werden können.

Die Zielsetzungen von FIDeS beinhalten unter anderem die interaktive Assistenz bei der Abwehr von Angriffen, Risikoanalysen und deklarative Beschreibungen und Erklärungen

der Angriffsmuster und deren Ursachen. Die KI soll soweit entwickelt und trainiert werden, dass sie aus dem Datenstrom erkannte Muster auch selbständig als gut- oder böseartig klassifizieren kann.

Und irgendwann wird es vielleicht auch eine einheitliche und praktikable Lösung für die heimische Kommunikation und sichere Datennutzung geben. Für Unternehmen jedenfalls stehen Dienstleister wie die nicos AG (www.nicos-ag.com), die sich auch an der Entwicklung von FIDeS beteiligt, schon mit elaborierten Businesslösungen parat.

Autor:

nicos AG
Thomas Brosch, Vorstand
Mendelstrasse 11
Technologiehof Münster
D-48149 Münster

info at nicos-ag.com
www.nicos-ag.com

Foto: Quelle-Dark Vectorangel/Fotolia.com

- Verwandte Themen
- .11n WLAN Bridge Out-of-the-box
- Anwendungen für den Einzelhandel auf der Grundlage sicherer IP- und Wireless-Technologien
- SonicWALL: Die besten Vorgehensweisen bei der Einrichtung eines sicheren Wireless-Netzwerks

Copyright All-About-Security.de / www.all-about-security.de Alle Rechte vorbehalten
Vervielfältigung nur mit Genehmigung von All-About-Security.de