

„Wir-kennen-uns-vertraue-mir“ – das Modell hat ausgedient“

VDI nachrichten, Düsseldorf, 2. 2. 07, swe –

Nach der Übernahme des ehemaligen Internet- und Netzwerk-giganten MCI im letzten Jahr und damit dessen Geschäfts mit global agierenden Unternehmen spielt der US-Telekommunikationskonzern Verizon Communications auch international vorn mit. Die Sicherheit der Netze ist für die Firmenkunden essentiell wichtig. Dennoch fehlt oft die Stringenz und ein längst nötiger Sinneswandel in den Unternehmen, um Informationssicherheit wirklich erreichen zu können, meint Sara Santarelli, die bei Verizons Business-Sparte für die Informationssicherheit zuständig ist.

Sara Santarelli ist es gewohnt mit Kunden umzugehen, die höchste Sicherheit für ihre Daten erwarten. Die Industrieingenieurin in Diensten von Verizon Business, der ehemaligen MCI, arbeitet in den USA direkt mit Kunden wie dem Department of Homeland Security oder globalen Konzernen wie DaimlerChrysler zusammen.

„Man kann die Vertraulichkeit von Daten nicht mit reiner Technologie erreichen“, wirbt sie für weniger Technikgläubigkeit. Santarelli, Chief Information Security Officer bei Verizon Business, verantwortet nicht nur die Datensicherheit für die rund 130 000 Kundenbeziehungen weltweit, sondern auch auf dem nach eigenen Angaben weltweit größten öffentlichen IP-Backbone.

„Das ‚Wir-kennen-uns-vertraue-mir‘-Modell hat ausgedient“, sagt sie, die Bedrohungen seien inzwischen zu vielfältig und weiteten sich durch mobile Geräte wie Smartphones zeitweilig aus. Diese seien bisher oft nicht in den Sicherheitskonzepten der Unternehmen vorgesehen.

Die Qualität der Angriffe habe sich verschärft: „Die Bedrohung bewegt sich hin zu einem Diebstahls-geschäft.“ Diebstahl von Konstruktions- und Forschungsdaten, Finanzdaten, Personal-

„Meine Theorie ist die, dass nur sehr, sehr wenige Leute Persönlichkeitsdaten auf einem Laptop, einem Mobilfunktelefon, einem PC oder einem

Mainframe wirklich benötigen. Deshalb müssen wir das Problem an der Wurzel packen, und das sind die Daten und wer darauf Zugriff hat.“

„Sicherheit muss durch ein Modell für die Verletzlichkeit der Sicherheitsbelange gemangelt werden“, beschreibt sie das Konzept, das Verizon Business den eigenen Kunden anbietet. „Es ist wichtig, dass alle Parteien im Unternehmen am Aufbau der Sicherheitsrichtlinien beteiligt sind. Das nachher überall in den Abteilungen einzeln zu kommunizieren ist unmöglich“, betont sie.

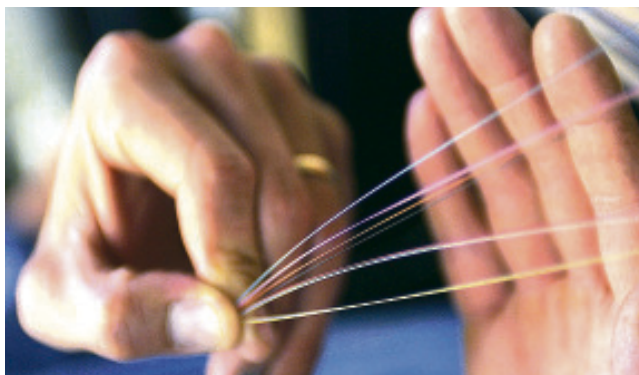
Wichtig sei dabei für viele Entscheider, dass es eine Metrik, eine Art Sicherheitsindex gibt, an dem sich der momentane Sicherheitszustand des Unternehmens messen lässt.

„Diese Metrik ist ein kritischer Teil bei der Kontrolle der Sicherheitsrichtlinien“, sagt Santarelli. Sie habe ihre eigene Metrik entwickelt. Verizon Business arbeitet mit einem Faktor für die Sicherheitslast, die von den jeweiligen Daten abhängt und dem gewählten Datenzugang abhängt.

Einen Risikomanagementprozess hatte sich Verizon Communications, der Mutterkonzern von Verizon Business, nach einem Zwischenfall im April 2005 selbst auferlegt. Ein Laptop mit vertraulichen Geschäftsdaten wurde in einer Tiefgarage aus dem Auto gestohlen. „Danach haben wir alle Daten inventarisiert.“ Heute ist der Zugang zu vertraulichen Daten stark beschränkt, die Daten auf Festplatten verschlüsselt.



Sara Santarelli: Die Chefin für Informationssicherheit bei Verizon Business hält gelebte Sicherheitskonzepte für unabdingbar. Foto: Verizon



Glasfasernetz als Grundlage: Verizon Business betreibt ein riesiges öffentliches Kernnetz auf Internet-Protocol-Basis. 60 Mio. Sicherheitsmeldungen laufen dort auf – täglich. Foto: dpa

Im IP-Netz von Verizon Business laufen täglich 60 Mio. Sicherheitsmeldungen auf, 1,6 Mio. IP-Adressen werden gescannt. „Jedes Jahr müssen wir jemanden anstellen, der unser Netzwerk nicht kennt und es testet. Das gibt uns Benchmarks.“

Im Marktgebiet von Europa, dem Mittleren Osten und Afrika (Emea) muss sich Verizon Business gegen Konkurrenten wie die British Telecom (BT) behaupten. „Emea ist ein sehr harter Markt“, räumt Santarelli ein, „aber es ist auch ein Wachstumsmarkt.“

Die eigene Stärke sei vor allem, dass

man sehr genau Bescheid wisse, was im eigenen IP-Backbone ablaufe und entsprechend sichere Netzbetriebe und integrierte Dienstleistungen für Unternehmenskunden anbieten könne. „Wir sind in der Lage genau zu sagen, wie sicher und stabil das zugrunde liegende Netzwerk ist und wie zufriedenstellend es läuft. Das ermöglicht uns eine sehr schnelle Diagnose, ob ein Fehler bei uns im Netzwerk liegt oder woanders.“

Für 2007 erhofft sich Santarelli, dass sich die Fusion von Verizon Communications mit seinem Mobilfunkbereich und MCI in entsprechend gebündelten, neuen Angeboten für die Unternehmenskunden bei Verizon Business niederschlägt.

„Unsere Planungen für den Sicherheitsbereich 2007 sind ambitioniert. Ich sehe da einen sehr starken Bedarf aus Emea kommen“, sagt sie. Europäische Kunden seien sehr besorgt um den Datenschutz und interessierten sich sehr für Wege und Empfehlungen zum Datenschutz.

Bisher, so Santarelli, habe sich die Fusion von Verizon und MCI ausgezahlt. Schließlich habe man zwei Kernnetze zusammenbringen müssen. „Der wichtigste Teil dabei ist die Analyse: Was brauche ich? Was macht den meisten Sinn? Dabei müssen natürlich der Kunde und seine Sicherheit immer im Vordergrund stehen.“

Verizon Communications Inc.

■ **Tätigkeitsfeld:** US-Telekommunikationskonzern, Festnetzgeschäft in den USA, Mobilfunkgeschäft Verizon Wireless (55 % hält Verizon, 45 % hält Vodafone), Verizon Business, globaler Netzbetrieb und Netzmanagement für Unternehmen (ehemals MCI).

■ **Umsatz*:** 88,144 Mrd. \$

■ **Gewinn*:** ca. 6,197 Mrd. \$

■ **Beschäftigte*:** 217 000

■ **Marktposition:** Gilt weltweit nach Umsatz als die Nr. 2 vor der Deutschen Telekom und hinter NTT.

www.verizon.com

*Geschäftsjahr 2006, Ende 31. 12. 2006
Quelle: ntr

STEPHAN W. EDER