



Nokia Siemens Networks

## Explosiv bis zum Schluss

Autor(en): Riem Sarsam

15.06.2007

**80 Manager atmen auf. Seit Juli 2006 haben sie das Joint Venture zwischen den Telefonnetzsparten von Siemens und Nokia verhandelt, abgeschirmt in einem eigens eingerichteten Datentresor. Dabei durfte nichts von den dort besprochenen Planungen nach außen dringen. Jetzt dürfen sie reden.**



Gemeinschaftsunternehmen Nokia Siemens Networks: Teammitglieder bewegen sich in einem explosiven Umfeld.

Lange durfte nichts über die neue Firma mit den 60.000 Mitarbeitern nach außen dringen. Die Spielregeln der Kartellbehörden sind eindeutig: "Bis zum endgültigen Abschluss sind beide Unternehmen Wettbewerber, die im gleichen Markt agieren", erklärt Alexander Littwin, Mitarbeiter der zentralen Strategieabteilung der Kommunikationssparte bei Siemens. Es darf keine öffentlichen Planungen zum künftigen und gemeinsamen Portfolio geben. Mit einer Ausnahme: Abstimmungen zur Produktplanung sind erlaubt, wenn sie besonders sicher stattfinden. In einem sogenannten Clean Team.

### Nur unter strengen Auflagen

Das Clean Team ist eine Auswahl aus Managern beider Unternehmen, die unter strengen Auflagen die künftige Ausrichtung des offiziell noch nicht existierenden Unternehmens diskutieren. "Das waren im Fall von Nokia Siemens Networks zu 80 Prozent Fragen des künftigen Produktportfolios, aber auch Planungen zu organisatorischen Zielstrukturen, die direkt mit der Produktstrategie zusammenhängen", berichtet Littwin, der zusammen mit spezialisierten Rechtsanwälten für den Aufbau und die Koordinierung des Clean Teams verantwortlich war. Mit der Einrichtung einer solchen Task Force versuchen die Unternehmen, Zeit zu gewinnen, denn gerade die kartellrechtlich untersagten Planungen zur künftigen Produktstrategie gehören zu den dringendsten. Die Kunden warten auf klare Ansagen von der neuen Nummer drei im weltweiten Geschäft für Netzausrüstung. Und mit jeder Verzögerung steigt die Gefahr, sie zur Konkurrenz zu treiben.

Insgesamt 80 hochrangige Manager, 40 von Nokia und 40 von Siemens, arbeiten seit Ende Juli vergangenen Jahres in dieser Gruppe. Jeder Einzelne unterzeichnete zuvor eine persönliche Vertraulichkeitserklärung mit strengen Auflagen. Weder an Kollegen noch an Kunden oder eine dritte Partei dürfen Informationen weitergegeben werden. Neben diesem Verbot sind außerdem der eingeschränkte E-Mail-Verkehr oder Datensicherheitsauflagen beschrieben. Besonders hart: Die Arbeit im Clean Team birgt für die Männer und Frauen ein persönliches Risiko. "Falls der Abschluss

doch nicht zustande kommt, dürfen die 80 Experten ein Jahr lang nicht in einem vergleichbaren Bereich arbeiten oder das Wissen aus der Zusammenarbeit weitergeben", sagt Littwin. Weder im eigenen Unternehmen noch bei der Konkurrenz.



Zweiter Anlauf: Aufrücken an die Spitze.

Auch für die Konzernmütter Nokia und **Siemens** beinhaltet eine derartige Verpflichtung Risiken. Bei Misslingen des Joint Ventures wären auf einen Schlag die führenden Köpfe in der Produktentwicklung für ein Jahr weg gewesen. "Das war besonders für einen Sektor, der so entwicklungsintensiv und dynamisch ist wie die Telekommunikation, eine wichtige Überlegung", erklärt Littwin. "Trotz des hohen Arbeitsaufwandes haben wir daher versucht, das Team möglichst klein zu halten, um so das Risiko für beide Unternehmen zu minimieren."

Um so mehr ging es daher im Clean Team um eine effiziente Erfüllung der Aufgabe. Man richtete in München und Helsinki separate Büros mit einer unabhängigen Infrastruktur ein. Die **IT-Systeme** waren nicht mit denen von **Siemens** oder Nokia verbunden und wurden auch nicht von einem der



Fakten zu **Siemens** Nokia

konzerneigenen Dienstleister betreut. Informationen, die in das Team hineingingen, und alles, was herauskam, unterlagen einer juristischen Prüfung. "Wir waren von einem Schutzschild von mehreren Rechtsanwälten abgeschirmt", erzählt Littwin. Diese legten auch fest, welche Themen relevant für die Arbeit im Team waren und welche nicht. "Alles, was mit Kunden und Produkten zusammenhängt, gehörte rein", erklärt der **Siemens**-Mann. Andere Themen,

etwa die künftige Mitarbeiterstruktur, konnten auch außerhalb des Teams erläutert werden. Diese Trennung ist zwar künstlich, denn die Festlegung auf bestimmte Produkte, ihre Herstellung und Vermarktung wirkt natürlich auf die gesamte Organisation. Für die 80-Mann-Truppe durfte dies jedoch keine Rolle spielen.

### Sicherheit im Datentresor

Für sie ging es vor allem darum, sich ein detailliertes Bild vom künftigen Partner zu verschaffen, speziell von dessen Produktportfolio. Beschreibungen in Datenblättern waren da noch das Unspektakulärste. Richtig spannend wurde es beispielsweise, wenn auf den Tisch kam, wie die Pläne zu seiner Weiterentwicklung der Produkte aussehen oder welche Kunden es wo einsetzen. Erst mit diesem Wissen konnten die Produktexperten und Entwicklungsmanager schließlich entscheiden, welche Produkte Nokia **Siemens** Networks auch auf lange Sicht weiter anbieten will.

Um den Informationsaustausch zwischen Finnland und Deutschland bei hohem Sicherheitsstandard zu gewährleisten, half ein virtueller Raum: Tresor, eine Software, die eigens für die Bearbeitung und den

Austausch kritischer Daten konzipiert wurde. Über diese Web-basierte Plattform bearbeiteten die Verantwortlichen sämtliche relevanten Dokumente, immer mit der Kontrolle darüber, wer was wann gelesen oder bearbeitet hat.

Die Lösung der Münchener Brainloop AG lässt sich im Unternehmen implementieren oder als ASP (**Application Service Providing**) nutzen. Für Letzteres entschied sich das Nokia-Siemens-Team. Sein Datentresor liegt auf einem **Server** von **T-Systems**. Die Vorteile eines gehosteten Systems waren Zeit, Geld und Sicherheit. Beispielsweise beim Zugriff auf die Informationen. Da es zwischen Nokia und **Siemens** keinen verschlüsselten E-Mail-Verkehr gab, hätte dieser erst aufgebaut werden müssen. "Das wäre in der vorhandenen Kürze nur mit höheren Kosten zu schaffen gewesen", sagt Littwin.

Und es ließ sich schneller arbeiten. Da die Daten für alle Beteiligten auf dem zentralen Server bereitliegen, lassen sie sich leicht und schnell aufrufen, egal zu welcher Zeit und von welchem Ort aus. "E-Mail-Anhänge, die erst durch das Filtersystem müssen, hätten wir nicht so schnell einsehen können", ist Littwin überzeugt.

### **Abfotografieren nicht möglich**

Gesichert wird der Zugriff auf das System durch eine Zwei-Faktoren-Authentifizierung: Neben dem üblichen Software-**Password** fungiert beim Nokia-Siemens-Team das Mobiltelefon mit SMS-Einmalschlüsseln als weiterer Token. Dabei erzeugt das System nach der klassischen Anmeldung per Kennwort eine sechsstellige Buchstaben-Kombination und schickt sie an das **Handy** der jeweiligen Person.

Wichtigstes Instrument ist allerdings das Archiv des Systems mit einer detaillierten Verwaltung der Zugriffsberechtigungen. Hier liegen die Dokumente mit den wesentlichen Informationen über ihre Nutzer und ihre Nutzung. Automatisch erzeugte Protokolle machen sämtliche Veränderungen in den Daten sichtbar und nachvollziehbar. Verschiedene Technologien verhindern das Herunterladen, Abfotografieren oder einen Screen Shot. Und eine spezielle Wasserzeichentechnik blockiert das unbefugte Weiterleiten der Dokumente. Einer Stichprobe durch die Kartellbehörden hätten diese Vorkehrungen standgehalten. Und es gab auch eine psychische Wirkung für die Beteiligten. Denn nicht zuletzt war es dieses Umfeld, meint Littwin, das die Teammitglieder immer wieder daran erinnerte, in welchem explosivem Umfeld sie sich bewegten.

<http://www.cio.de/strategien/methoden/834804/index3.html>