

REMOTE ACCESS VPN „OUT OF THE CLOUD“

„Mobile Telearbeit via Internet“ im Landesverwaltungsnetz Nordrhein-Westfalen

Der Landesbetrieb Information und Technik Nordrhein-Westfalen (IT.NRW) bietet rund 40.000 Beschäftigten der Landesverwaltung die Möglichkeit, nicht nur vom stationären, sondern auch vom Telearbeitsplatz sicher und kostengünstig auf die dienstlich benötigten Informationen zugreifen zu können. Durch den Einsatz einer mandantenfähigen Virtual Private Network (VPN)-Lösung von NCP wurde eine „Private Cloud“ - ein speziell geschaltetes und geschütztes Netzwerk – aufgebaut, in dem ausschließlich die dort angeschlossenen personalisierten Teilnehmerinnen und Teilnehmer kommunizieren und Zugang über das Internet zu ihrem jeweiligen Behördennetz erhalten.

IT.NRW ist am 01.01.2009 durch die Zusammenführung des ehemaligen Landesamtes für Datenverarbeitung und Statistik Nordrhein-Westfalen (LDS NRW) mit den gemeinsamen Gebietsrechenzentren (GGRZ) Hagen, Köln und Münster entstanden und beschäftigt derzeit 2.200 Mitarbeiterinnen und Mitarbeiter. Der Betriebssitz ist Düsseldorf mit Standorten in Oberhausen, Paderborn, Hagen, Köln und Münster. IT.NRW vereint alle klassischen Funktionen eines MSSP-Dienstleisters (Managed Security Service Provider) und betreibt im Auftrag des Ministeriums für Inneres und Kommunales Nordrhein-Westfalen

die zentrale Infrastruktur. Weiter stellt IT.NRW alle Service-Leistungen zur Einrichtung und zum Support der Telearbeit zur Verfügung. In Anspruch nehmen können den Service von IT.NRW alle Behörden und Einrichtungen des Landes, die an das Landesverwaltungsnetz (LVN) angeschlossen sind.

Das LVN ist eine Netzinfrastruktur, unterteilt in viele Subnetze, über die alle Behörden und Einrichtungen der Landesverwaltung Nordrhein-Westfalen ihre Datenkommunikation abwickeln können. Regional in Nordrhein-Westfalen verteilte Netzknoten, die über schnelle Leitungen miteinander verbunden sind, bilden die technische Netzbasis. Für jede LVN-Teilnehmerin und jeden LVN-Teilnehmer ist ein eigener, abgesicherter Bereich reserviert und der Datenfluss wird über individuell konfigurierte Kommunikationsbeziehungen geregelt. Damit ist Diskretion innerhalb des Kundennetzes garantiert.

„IT.NRW bietet einen komplett transparenten Netzwerkzugang. Unsere Kunden benötigen nur einen Anschluss an das gemeinsame Netz, um ihre Kommunikationspartner innerhalb und außerhalb der Landesverwaltung sowie das Internet zu erreichen. Indem wir das Internet als Transportmedium nutzen, vermeiden wir den Einsatz teurer Leitungen – wie bspw. ISDN-Wählverbindungen – und können auch abgelegene Verwaltungseinheiten einbinden, ohne dass hohe Verbindungsgebühren entstehen“,

erklärt Roger Schwentker, verantwortlicher Referent für die VPN-Lösung bei IT.NRW.

Hochsicher und mandantenfähig

Für die Umsetzung des Betriebskonzeptes wurden Sicherheits- und funktionale Anforderungen definiert. Diese Kommunikationsrichtlinien legen die Rahmenbedingungen für die Weiterentwicklung und den Betrieb der Kommunikationsinfrastruktur der Landesverwaltung fest und regeln ihre Nutzung.

Der Einsatz von IT-Lösungen im Bereich der Landesverwaltung bedingt hohe Ansprüche an die Sicherheit und Qualität aller eingesetzten Systemkomponenten.

Vorteile für IT.NRW:

- ▶ softwarebasierte, virtualisierbare VPN-Lösung
- ▶ Mandantenfähigkeit
- ▶ Single Point of Administration
- ▶ geringe Betriebskosten
- ▶ geringer Personalaufwand
- ▶ geringer Schulungsaufwand
- ▶ preiswertes Angebot

Vorteile für den Kunden:

- ▶ geringe Investitionen in Hardware, Software und Expertenwissen im eigenen Haus
- ▶ schnelle Implementierung
- ▶ hohe Skalierbarkeit
- ▶ ausgereifte Technologie
- ▶ Infrastruktur mit hoher Verfügbarkeit und Datensicherheit

IT.NRW suchte daher nach einer Remote Access-Lösung, die es aufgrund ihrer Architektur und Funktionen sowohl server- als auch clientseitig ermöglicht, den Sicherheitslevel auf höchstem Niveau zu halten. Um dies in einem Netzwerk mit mehreren tausend Anwenderinnen und Anwendern gewährleisten zu können, spielen auch die Bedienbarkeit und das

„DIE ADMINISTRATION DER DERZEIT 4.000 TELEARBEITER FINDET DANK DES NCP SECURE ENTERPRISE MANGEMENTS NAHEZU VOLLAUTOMATISCH STATT“

Roger Schwentker,
IT.NRW

Management der Remote Access-Lösung eine entscheidende Rolle. Vorgabe war, dass der Umgang mit der VPN-Software für den Anwender einfach zu handhaben ist und die Verbindung zum Firmennetz und dessen Security Infrastruktur ausschließlich über einen VPN-Tunnel erfolgen muss. Zudem sollten sämtliche Kommunikations- und Sicherheitsparameter in einer zentralen Management Komponente zusammengefasst sein.

In Remote Access-Strukturen wie bei IT.NRW, in denen mehrere Kunden gemeinsam eine VPN-Plattform nutzen, war die „Mandantenfähigkeit“ des Systems eine weitere Vorgabe. Die Lösung musste in der Lage sein, auf nur einem Server oder Software-System mehrere Kunden parallel zu bedienen und dabei die Datenströme strikt voneinander getrennt zu halten.

Nach der Evaluierung verschiedener Produkte entschied man sich für die VPN-Lösung der NCP engineering GmbH. Der Nürnberger Remote Access-Spezialist ist seit Jahren anerkannter Technologielieferant nicht nur für Behörden und Ministerien. Auf Basis seiner „Next Generation Network Access Technology“ bietet das Unternehmen eine universelle,

zentral administrierbare Remote Access VPN-Lösung.

Mit nur einem Klick im Netz

Begeistert sind Schwentker und sein Team von der NCP Secure Enterprise Client Suite, die auf den Endgeräten der Telearbeiterinnen und -arbeiter zum Einsatz kommt: „Traditionelle VPN-Clients kümmern sich ausschließlich um den VPN-Tunnel und setzen „stillschweigend“ voraus, dass die Anwenderinnen bzw. der Anwender bereits erfolgreich eine Internetwahl hergestellt hat. Die Erfahrung zeigt jedoch, dass gerade an dieser Stelle unendlich viele Fehlerquellen lauern. Die NCP-Software erledigt mit einem einzigen Klick die Einwahl ins Internet, den Aufbau des VPN-Tunnels und in Abhängigkeit von der jeweiligen Remote Access-Umgebung die Auswahl der richtigen Firewall-Regel.“

Bevor die Benutzerinnen bzw. Benutzer jedoch Zugang in das geschützte LVN erhalten, müssen sie sich mit „Besitz und Wissen“ authentisieren. Dies erfolgt über eine SmartCard (Besitz), die diese Telebeschäftigten zusammen mit der VPN-Software erhalten. Auf dieser ist der Schlüssel für den virtuellen Eintritt ins LVN sicher abgelegt. Die Freigabe dieses Schlüssels erfolgt über die Eingabe eines Passwortes (Wissen). Nach erfolgreicher Authentisierung baut

der VPN-Client einen transparenten VPN-Tunnel auf, d. h., dem User stehen am Telearbeitsplatz über die NCP Secure Client Suite alle Netzwerkanwendungen und -funktionalitäten wie im Büro zur Verfügung.

Als Gegenstelle zu den VPN-Clients ist bei allen Kunden ein NCP Secure Enterprise VPN Server installiert. Im Düsseldorfer Rechenzentrum von IT.NRW befindet sich ein redundant ausgelegtes VPN-Server-System sowie das NCP Secure Enterprise Management (SEM). Der VPN-Server übernimmt die Überprüfung (Authentisierung) der VPN-Benutzer, die Terminierung des VPN-Tunnels sowie die Weiterleitung der Verbindung durch weitere Tunnel in die jeweiligen Kundennetze. Die Architektur des VPN-Servers ist auf hohe Skalierbarkeit ausgelegt, sodass IT.NRW die Anzahl der Mandanten jederzeit dem aktuellen Bedarf anpassen kann.

Komfort für Administratoren und Telebeschäftigten

Für Administratoren fallen bei einem VPN-Betrieb dieser Größenordnung viele Tätigkeiten an, die überwacht und angestoßen werden müssen. Dazu gehören die Verwaltung des VPN-Gateways, das zentrale Verteilen und Aktualisieren der Client-Software, das Management der Ausgabe für digitale Software- oder Hardwarezertifikate, die SEM-Konsole hinsichtlich Identitäts- und



Rechte-Management sowie die Sicherheitsüberprüfung der Endgeräte (Endpoint Security) vor deren Zugriff auf das LVN. Mit dem NCP Secure Enterprise Management steht Schwentker und seinem Team ein leistungsstarkes System zur Verfügung. Über nur eine Konsole lassen sich sämtliche Tätigkeiten komfortabel steuern. So können beispielsweise komplette Gruppen beziehungsweise deren Benutzerprofile mithilfe eines Vorlagenkonzepts mit nur wenigen Klicks aktualisiert werden. Jedes Update läuft beim Kunden vollautomatisch ab. Sobald sich die Telearbeiterin bzw. der Telearbeiter mit seinem Zielnetz verbindet, informiert ein zusätzliches Bildschirmfenster über ein anstehendes Update für den eingeloggten PC.

Die Konfigurations-Parameter der VPN Client Suite werden von zentraler Stelle so angelegt, dass sie von der Anwenderin bzw. vom Anwender nicht umgeh- bzw. manipulierbar sind. „Diese Parametersperren lassen sich granular definieren. Somit können wir präzise Zugriffsschutzlisten

„NCP hat es wirklich geschafft, die Bedienbarkeit des Clients so einfach wie ein Telefongespräch zu gestalten“

**Roger Schwentker,
IT.NRW**

erstellen und verhindern gleichzeitig eine gewollte oder ungewollte Fehlkonfiguration des VPN-Clients durch die User. Das entlastet den Helpdesk enorm“, so Schwentker.

Für die Telebeschäftigten wurde die Bedienung dahingehend weiter vereinfacht, dass nicht relevante Menüs und Einstellungsmöglichkeiten ausgeblendet wurden und sie sich somit nicht mit unterschiedlichen

Software-Oberflächen auseinanderzusetzen müssen.

IT.NRW richtet sein Dienstleistungsangebot flexibel an den Bedürfnissen der Kunden aus. Bei der Erstinstallation erhalten die Kunden Unterstützung bei der Installation der Client- und Server-Software sowie bei der Konfiguration der Linkprofile. Des Weiteren erfolgt eine umfassende Schulung der IT-Administratoren. IT.NRW bietet zusätzlich 2nd Level Support für die Clients und die VPN-Server der Kunden und fungiert als Schnittstelle zum 3rd Level Support durch NCP.

Inzwischen bedient IT.NRW 60 Kunden mit ihrer Remote Access VPN-Lösung, angefangen von Landesministerien, Bezirksregierungen bis hin zu Justizvollzugsanstalten, Umweltämtern und Forstbehörden etc. Herr Schwentker und sein Team haben das VPN zu jeder Zeit „voll im Griff“ und der Kundenstamm wächst kontinuierlich. Die Kunden wissen die Vorteile eines gemanagten VPN zu schätzen. Die Infrastruktur – also alle rein technischen Probleme wie Verfügbarkeit, Datensicherung, Schutz vor Hackern usw. – muss nicht jedesmal neu gelöst werden, da es sich um einen etablierten Prozess handelt, der von IT.NRW zur Verfügung gestellt wird.

„Die VPN-Server laufen sehr stabil und die Administration der derzeit 40.000 Telearbeiterinnen und -arbeiter findet dank des NCP Secure Enterprise Managements nahezu vollautomatisch statt. Der Support-Aufwand für so eine große Anzahl an Usern ist im Verhältnis minimal. Und NCP hat es wirklich geschafft, die Bedienbarkeit des Clients so einfach wie ein Telefongespräch zu gestalten“, resümiert Schwentker.

Um die Verfügbarkeit der Infrastruktur weiter zu optimieren

ist eine redundante, verteilte Auslegung der Datenzentren geplant. Hierfür werden zusätzliche Secure Enterprise VPN Server in den Standort-Rechenzentren Hagen und/oder Münster installiert, deren Verwaltung ebenfalls über das SEM läuft. Erste Tests laufen bereits. Den Client betreffend ist zum einen die Migration von Windows®XP auf Windows®7 in Planung, zum anderen sollen Untersuchungen stattfinden, was den Bedarf an Linux oder Thin-Clients betrifft.

Über NCP engineering, GmbH

Die NCP engineering GmbH ist Hersteller von Softwarelösungen für die hochsichere Unternehmenskommunikation über öffentliche Netze und das Internet. NCPs Kernkompetenzen liegen auf den Gebieten Remote Access, IP-Routing, VPN und Firewall Technologien, Identity und Access Management (IAM), Network Access Control (NAC) sowie Strong Authentication und Integration von PKI-Infrastrukturen. Einfache Bedienung, zentrales Management, Kompatibilität und Wirtschaftlichkeit sind wesentliche Eigenschaften der NCP-Lösung. Die Integration in bereits bestehende IT-Infrastrukturen ist problemlos möglich.