SecurITy made in Germany
Trust Seal
www.teletrust.de/itsmig

NCP
SECURE COMMUNICATIONS

Case Study

Remote Access als Full Managed Service bei der Ratiodata SE

Remote Access als Full Managed Service – die Ratiodata SE macht es vor

Auch Sicherheits-Services wie ein Virtual Private Network (VPN) lassen sich heute in die Cloud auslagern. Ein Anbieter, der sich bereits vor Jahren hierauf spezialisiert hat und zusätzlich über branchenspezifisches Knowhow in der Finanzindustrie verfügt, ist die Ratiodata SE, der Systemhauspartner der Genossenschaftlichen FinanzGruppe und eine hundertprozentige Tochter von Atruvia AG. Die Ratiodata Gruppe beschäftigt an 11 Standorten und 16 Campus-Teams in ganz Deutschland rund 1.500 Mitarbeiter.

Das Unternehmen erfüllt alle Maßgaben des Gesetzgebers und der Finanzdienstleister bezüglich der besonderen branchenbezogenen IT-Anforderungen und ist als eines der großen Systemhäuser in Deutschland im Segment Bankentechnologie sogar der Marktführer für herstellerunabhängigen Service.

Das Portfolio an Produkten und Dienstleistungen umfasst unter anderem das Management und bundesweite Services rund um die stationäre und mobile IT-Infrastruktur, die Arbeitsplatzausstattung sowie Netzwerk- und Sicherheitslösungen.

Ihre Dienstleistungen und Services bietet die Ratiodata Unternehmen der Genossenschaftlichen FinanzGruppe sowie Marktkunden u. a. aus dem Bereich Healthcare an. So arbeitet sie derzeit u. a. für die Unternehmen der DZ Bank Gruppe und die Mitgliedsbanken sowie weitere Kunden von Atruvia AG.

Sicherer und hochverfügbarer Zugang

Der Remote Access Service (RAS) der Ratiodata bietet den Kunden einen sicheren und hochverfügbaren Zugang zu internen Netzen und Applikationen, unabhängig vom jeweiligen Zugangsweg und Aufenthaltsort eines Mitarbeiters. Durch den Einsatz von hard- bzw. softwarebasierten Sicherheitszertifikaten für die Nutzer-Authentifizierung und durch die Verschlüsselung sämtlicher Daten bietet der RAS ein Höchstmaß an Sicherheit.

Mandantenfähige Remote Access Plattform

Die Ratiodata (Anmerkung: damals noch als VR Netze) hat den Einsatz der IPsec VPN Technologie von NCP bereits im Jahr 2000 aufgenommen – damals wurden sechs NCP Secure Enterprise VPN Server dazu genutzt, rund 7.000 Nutzern Remote Access zur Verfügung zu stellen. Bis heute wurde der Service auf **24 Systeme** ausgeweitet, über die **35.000 Nutzer** von externen Standorten in Deutschland und weltweit auf das Netzwerk zugreifen.

Die Anforderungen konnten durch die Remote Access Lösung von NCP für verschiedene IP-fähige Endgeräte umgesetzt werden. Weitere Merkmale der Remote Access Lösung sind zertifikatsbasierte Authentifizierung (USB-Token, Softzertifikate, Smartcard) in einer PKI (Entrust CA) und einer **IPSec VPN-Infrastruktur mit NCP Secure Enterprise Clients (Win32/64), mehreren NCP Secure Enterprise VPN Servern**, NCP Secure Enterprise Load Balancing Server und dem NCP Secure Enterprise Management.

Überzeugender Lösungsansatz

Zur Entscheidungsfindung für die NCP-Lösung haben laut Ratiodata die Hochskalierbarkeit der Plattform, die Nutzerfreundlichkeit in der Verwaltung und im Betrieb für Administratoren durch das zentrale VPN Management sowie die breite Kompatibilität zu unterschiedlichen Plattformen und Betriebssystemen beigetragen. Gefordert war und ist noch immer eine Unterstützung von Linux, verschiedene jeweils supportete aktuelle Windows-Versionen und Mac-OS, die bei nur wenigen anderen Anbietern zu finden war.

Ein weiteres Entscheidungskriterium waren mehrere technologische Alleinstellungsmerkmale, welche die Lösung zu einem All-In-One-Paket für Security und Remote Access Anforderungen machen: Die leistungsstarke integrierte Personal Firewall für jedes Endgerät, Endpoint Security Checks, der integrierte Dialer zur Auswahl des leistungsstärksten Kommunikationskanals und die mehrsprachige Benutzeroberfläche für internationale Clients. Hinzu kam die Anforderung, dass die Software alle Verbindungsmedien unterstützen sollte – WLAN an Hot Spots, **mobiler LTE-Zugang** und direkte Unterstützung von GPRS/UMTS Karten, inklusive der Reduzierung des Datenvolumentransfers durch Komprimierung als seinerzeit wichtigen Kostensenkungsfaktor.

Vorteile

Die Erfahrung beim Einsatz der IPsec VPN Technologie von NCP hat gezeigt, dass alle funktionalen Anforderungen der Ratiodata sowie die ihrer Mandanten erfüllt werden konnten, wie zum Beispiel die Integration digitaler Zertifikate für ein höheres Sicherheitslevel bei der Nutzerauthentifizierung. Die Lösung hat die Aufwände beim Verwalten einer so großen Installation signifikant reduziert. Dies erlaubte es der Ratiodata in der Folge von beträchtlichen Einsparungen im Zusammenhang mit Schulungen und dem Support von Nutzern und Administratoren zu profitieren.

Die integrierte Personal Firewall mit ihren zahlreichen Konfigurationsmöglichkeiten und den damit abgesicherten Nutzerszenarien in der Praxis sowie der Load Balancing Server für Hochverfügbarkeit des Systems konnten ebenfalls zu Einsparungen beitragen, da eine Anschaffung weiterer Security Hardware- Komponenten aufgrund des hohen Sicherheitslevels der Lösung nicht notwendig war.

- ☑ Mandantenfähigkeit
- ☑ Hochverfügbarkeit durch Load Balancing Server
- ☑ Leistungsstarke, integrierte Personal Firewall für jedes Endgerät
- ☑ Endpoint Security Checks
- ☑ Mehrsprachige Benutzeroberfläche
- ☑ Reduzierte Aufwände beim Verwalten großer Installationen
- ☑ Einsparungen im Bereich Training und Support

Gewachsene Anforderungen – Hotspots, TrustSec, K-Fall-Schutz

Die Nutzerzahlen sind seit dem Aufbau der Plattform stark gestiegen. Ebenso wird der Service im Homeoffice und dank aktueller Funktarife und verbreiteter öffentlicher WLANs an externen Standorten in viel größerem Maße genutzt, als dies noch vor wenigen Jahren der Fall war. Dem hat die Ratiodata durch Erweiterung der Gateway-Plattform auf heute **24 Servern** Rechnung getragen. Dabei profitierte man auch von der erheblichen Leistungssteigerung der NCP Gateway Software.

In Hotels und anderen öffentlichen Räumen sind die dort zur Nutzung bereitgestellten ISDN-Anschlüsse längst WLAN-Zugängen mit individueller Authentifizierung gewichen. Die Anmeldung an derartigen Hotspots unterstützt die NCP-Lösung durch ein Zusammenspiel aus einem separaten Browser mit kurzfristiger Firewallöffnung. So können die Kunden ohne Modifikation an der Konfiguration der eigenen Services, etwa an der Browser-Konfiguration oder der Proxy-Einstellung, ihren Mitarbeitern auch diesen verbreiteten Zugangsweg bereitstellen.

Auch sehr spezielle Kundenszenarien ließen sich mit der NCP-Lösung elegant umsetzen. Dazu gehört das Security-Tagging TrustSec von Cisco, bei dem der Client abhängig von der Sicherheitseinstufung im AD des Kunden einem Adresspool zugeordnet wird, der am Netzeingang mit der vorgesehenen Sicherheitsstufe identifiziert wird.

Um Sicherheit geht es auch bei der Behandlung des Themas K-Fall und Pandemie. Vorfälle wie die „Schweinegrippe", die „Corona-Pandemie" oder „Blockupy" führten dazu, dass schlagartig ein erheblicher Mitarbeiteranteil vom Homeoffice als RAS-User arbeiten musste. Flexible Lizenzoptionen erlauben es, dies den Kunden im Notfall zu ermöglichen, ohne für jeden potenziellen User den Service zu buchen.

Service für unterschiedliche Mandanten

Zu Beginn der Zusammenarbeit rät **Frank Waldschmidt** von der Ratiodata als Serviceanbieter seinen Kunden dazu, sich die Einsatzumgebungen ihrer Mitarbeiter genau anzusehen und sich Gedanken über mögliche Nutzungsszenarien zu machen.

> *„Es geht nicht nur um die Anzahl der Anwender, sondern auch um die Umgebung, in der sie ihre Endgeräte einsetzen. Wo liegen die Daten, auf die die Unternehmen zugreifen müssen? Auch die zunehmende Nutzung von Cloud Services durch die Kunden gilt es zu berücksichtigen. Hier bieten wir mit dem NCP-Client unseren Kunden mittels Split Tunneling und VPN-Bypass intelligente Funktionen, um ein hybrides Cloud-Modell zu unterstützen."*
>
> ***Frank Waldschmidt, Ratiodata SE***

Daten über die dezentrale Infrastruktur sammelt die Ratiodata am Anfang gemeinsam mit dem Kunden, beispielsweise die Anzahl der Anwender sowie die Art der Endgeräte und Betriebssysteme im Einsatz. Je nach VPN-Lösung müssen die verwendeten Betriebssysteme und Versionen mit den VPN-Clients kompatibel sein.

Darüber hinaus werden Angaben über die Einbindung in die Directory- und Metadirectory-Strukturen des Kunden benötigt, um z.B. bei einer Integration in Active Directory unterschiedliche Remote-Access-Berechtigungen an einzelne Nutzer und Gruppen zu vergeben. Als Serviceprovider passt sich die Ratiodata bei diesen Verwaltungsprozessen an ihre Kunden an. In der Regel wird das Active Directory ausgelesen, aber auch Kopplungen zu HR-Software sind möglich und wurden bereits umgesetzt.

„Wir versuchen das immer automatisiert zu lösen und uns an die zentrale User-Datenbank zu hängen. Wie man das auch immer technisch löst, es muss in die Kundenumgebung passen. Kleinere Unternehmen kaufen die Benutzerverwaltung in der Regel ein, die größeren wollen das gern selbst machen. Die haben oft komplette Abteilungen, die sich um die Benutzerverwaltung kümmern."

Frank Waldschmidt, Ratiodata SE

Der Kunde hat Mitwirkungspflicht und Verantwortung für die Daten

Auch bei späteren Änderungen stehen den Kunden mehrere Möglichkeiten offen, damit alle realen Fälle in der Praxis abgedeckt sind. Verlässt beispielsweise ein Mitarbeiter das Unternehmen oder wird ein neuer eingestellt, taucht die Änderung im Rahmen der regelmäßigen Synchronisation auf. In kleinen Installationen reicht häufig eine E-Mail an den Account-Manager oder ein standardisiertes Formular, in das der Change Request eingetragen wird.

Die Kunden haben durch einen festen Ansprechpartner immer auch eine vertraglich festgeschriebene Mitwirkungspflicht und können die Verantwortung nicht komplett an den Provider abgeben. Vor allem aus rechtlicher Sicht bleibt die Verantwortung für die Daten weiterhin beim Unternehmen selbst, d.h. es muss auch in der Zusammenarbeit mit einem Serviceprovider dafür Sorge tragen, dass persönliche Daten den Datenschutzbestimmungen gemäß behandelt werden.

Technischer Spagat beim Hosting verschiedener Kunden

Anfangs stellt die Verteilung der Client-Software noch eine maßgebliche Aufgabe dar. Hierfür nutzt die Ratiodata den NCP Secure Enterprise VPN Server (Gateway), bei dem die Verteilung Bestandteil der Managementplattform NCP Secure Enterprise Management (SEM) ist.

Aus der Erfahrung heraus wird die Verteiloption über SEM bevorzugt. Dann wird lediglich definiert, welche Gruppe das Update erhält und beim nächsten Anmelden über eine ausreichend schnelle Netzverbindung wird der Client heruntergeladen und installiert. Allerdings arbeitet die VPN-Lösung auch mit jeder anderen Distributionslösung.

Beim Hosting vieler Tausend VPN-Tunnel steht die Ratiodata vor der großen Herausforderung, hohe Lastanforderungen zu stemmen. Dies wird durch Skalierbarkeit und Load Balancing der Gateways in der Gesamtlösung gewährleistet. Eine Management-Konsole, die sowohl mit mehreren Gateways als auch mit getrennten Mandanten zurechtkommt, unterstützt die Prozesse des Anbieters und die Sicherheitsbedürfnisse der Kunden gleichermaßen. Ob diese ein geteiltes VPN-Gateway akzeptieren oder eine getrennte Lösung fordern, wird durch das jeweilige Sicherheitskonzept des Kunden bestimmt.

> *„Wir sind unter anderem nach ISO 27001 und IDW PS 951 TYP 2 zertifiziert und hosten unsere Lösung über zwei redundant angebundene Rechenzentren. Davon profitieren auch Kunden, die eigentlich geringere Ansprüche an die Verfügbarkeit stellen würden."*
>
> ***Frank Waldschmidt, Ratiodata SE***

Wegen ihrer Spezialisierung auf den Finanzsektor und damit hoher spezieller Compliance-Vorgaben, nutzt die Ratiodata für ihre Lösung eine redundante Ausführung von Gateways und Netzzugängen.
Auch die VPN-Gateways sind redundant und über ein Hochverfügbarkeitsprotokoll verbunden, sodass sie Load-Sharing unterstützen.

Über NCP engineering GmbH

Die NCP engineering GmbH mit Hauptsitz in Nürnberg konzentriert sich seit über 35 Jahren auf die Entwicklung universell einsetzbarer Software-Komponenten für die einfache und sichere Vernetzung von Endgeräten und Systemen über öffentliche Netze. Eingesetzt wer-den die Secure Communications Lösungen in den Bereichen IIoT / Industrie 4.0 / M2M sowie Mobile Computing und Filialvernetzung. NCPs Kernkompetenzen sind zentrales, vollautomatisiertes VPN Management sowie Verschlüsselungs- und Firewall-Technologien.

Einfache Bedienung, zentrales Management, Kompatibilität und Wirtschaftlichkeit sind wesentliche Eigenschaften der NCP-Lösung. Die Integration in bereits bestehende IT-Infrastrukturen ist problemlos möglich.

NCP
SECURE COMMUNICATIONS

Sie haben Fragen oder möchten einen Termin für eine Produktdemonstration vereinbaren? Dann kontaktieren Sie uns!

NCP engineering GmbH
Dombühler Straße 2
90449 Nürnberg

Tel.: +49 911 9968-0
vertrieb@ncp-e.com
www.ncp-e.com

Wir freuen uns auf ein Gespräch mit Ihnen!