Quelle: E-Paper Kampagne "Digitalisierung jetzt! - Produktion & Fertigung" in der FAZ Digital & FAZ Kiosk aus dem unabhängigen Verlagshaus Mediaplanet Deutschland

Schnell, sicher und skalierbar – IT-Lösungen von NCP

Hohe Skalierbarkeit und Nutzerfreundlichkeit, breite Kompatibilität sowie sichere digitale Kommunikation – das sind nur ein paar Voraussetzungen der Ratiodata für ihre passgenauen IT-Lösungen im herausfordernden Umfeld der Finanzindustrie. Ein Gespräch erklärt Frank Waldschmidt, Leiter Network Engineering Mobility, wie all das mit den innovativen Services des Geschäftspartners NCP sogar in Zeiten einer Coronakrise und Tausender Mitarbeiter im Homeoffice gelingt.

Text Dominik Maaßen

Frank Waldschmidt
Leiter Network Engineering Mobility, Ratiodata GmbH

Dieser Artikel ist in **Zusammenarbeit mit NCP** entstanden.

Sie vertrauen schon länger den Lösungen von NCP – warum und von welchen Vorteilen profitieren Sie dabei?
Wir sind ein IT-Systemhaus und ein Großteil unserer Kunden kommt aus der Finanzbranche. Deshalb sind sichere und skalierbare Lösungen bei uns der Standard. Wir haben uns bereits im Jahr 2000 für die Services von NCP entschieden. Denn wir schätzen die Vorteile eines Herstellers, der sich unter anderem auf das Thema Remote Access spezialisiert hat. Damit können wir auch individuelle Anforderungen unserer Kunden umsetzen.

Diese geben spezielle Rahmenbedingungen, wie die strengen Vorgaben der BaFin oder der EZB, vor. Da ist es von Vorteil, dass wir NCP-Sicherheitslösungen eines deutschen Herstellers verwenden, den das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt.

In Sachen sichere digitale Kommunikation sind wir also speziell für die Finanzindustrie bestens gerüstet. Die Lösungen von NCP haben erweiterbare Security-Funktionen. Zu nennen sind hier die intelligente dynamische Firewall oder die Endpoint-Security-Funktionen. Letztere werten den Sicherheitsstatus des Gerätes auf. In einem Notfall können sie die VPN-Verbindung ins Firmennetzwerk entweder verhindern, oder es gibt vordefinierte Maßnahmen, um den Zugriff ausschließlich in ein spezielles Quarantänenetz vorzugeben. Wir scannen wöchentlich mögliche Schwachstellen und führen Penetrationstests mithilfe externer Spezialisten durch. Bei Unregelmäßigkeiten können wir wegen des hoch qualifizierten Supports schneller reagieren als so manch andere Unternehmen.

> Seit Anfang März arbeiten circa 20.000 der insgesamt 30.000 Anwender über die Umgebung von NCP permanent im Homeoffice – und das ohne Einschränkung oder Ausfälle.

ratiodata.de

Auch Sie sind zurzeit von der Coronakrise betroffen – wie helfen Ihnen die Lösungen gerade jetzt?
Seit Anfang März arbeiten circa 20.000 der insgesamt 30.000 Anwender über die Umgebung von NCP permanent im Homeoffice – und das ohne Einschränkung oder Ausfälle. Das ist das 1,5-Fache der normalen Nutzung. NCP hat uns und unseren Kunden ermöglicht, schnell und unkompliziert die Kapazitäten durch entsprechende Pandemie-Lizenzpakete zu erhöhen. Da die Lösung im Management bereits technisch sehr ausgereift ist, lässt sie sich problemlos erweitern. Wir können also leicht weitere Standard-Serversysteme integrieren oder Systemkonfigurationen verteilen. Das ist mit einer anderen Lösung auf der Basis einer speziellen Hardware schwer oder wegen Lieferengpässen überhaupt nicht möglich.

Wie praktisch ist die Software für den Mitarbeiter, der sie nutzt?
Die Lösung ist wegen ihres komfortablen VPN-Clients sehr einfach anzuwenden. Treten dennoch Störungen oder Fragen auf, helfen entsprechende Meldungen des Clients und ausführliche Logs. Da wir ein Serviceprovider sind, ist es jedoch mindestens genauso wichtig, dass wir die mandantenfähige Plattform von NCP um neue Funktionen oder Kunden erweitern können.

Wie profitiert am Ende Ihr Unternehmen davon?
Es ist und war schon immer unser Ziel, Lösungen nicht für jeden neuen Kunden separat erneut aufzubauen und zu betreiben. Wir brauchen Produkte, die durch gute Rollenkonzepte überzeugen und eine Multi-Mandantenlösung ermöglichen. Hier sehen wir die Services von NCP im Remote-Accesss-Umfeld als die für uns derzeit beste Lösung. ■

> Es wird eng im VPN-Tunnel: Mit einem Mal braucht es mehrere Tausend Lizenzen mehr, wenn der Zugriff dynamisch wächst. Anbieter arbeiten hier mit unterschiedlichen Modellen.

Unsichtbar im sicheren Tunnel

Parallel zur Zahl der Heimarbeiter steigen auch die Sicherheitsanforderungen der Unternehmen. Diese müssen nun plötzlich ihren zunehmenden Datenverkehr im VPN-Tunnel erweitern und managen.

Text Dominik Maaßen

Während Corona die Welt im Griff hat, stehen IT-Verantwortliche zurzeit vor noch mehr Herausforderungen als bisher: Denn um das Geschäft kontinuierlich am Laufen zu halten und die Gesundheit der Angestellten zu schützen, arbeiten nun Millionen von Mitarbeitern im Homeoffice. Allerdings sagt sich das so leicht. Viele Unternehmen müssen auf die Schnelle bei null starten und ihre Kapazitäten extrem hochfahren.

Sicherheit im Virtual Private Network

So gibt es in der IT ganz banale Fragen der Ausstattung wie Internetzugang oder mobile Endgeräte. Darüber hinaus muss die Tätigkeit gleichzeitig sicher sein, damit Hacker keinen Zugriff auf Daten erhalten. Cyberkriminelle sind schon in normalen Zeiten enorm erfolgreich, im turbulenten Krisenmodus öffnen sich für sie automatisch mehr Einfallstore.

Von diesem Bedarf profitieren momentan die VPN-Anbieter: Dank des Virtual Private Networks können Mitarbeiter und Unternehmen auf Dateien oder Software sicher zugreifen. Wie in einem gesicherten Tunnel kann der Angestellte damit eine verschlüsselte Verbindung zum Büronetzwerk herstellen. Außendienstmitarbeiter erhielten so zum Beispiel bisher Zugriff auf Dateien im Firmennetz, nun vermehrt die Kollegen im Home-Office. Für Außenstehende, wie zum Beispiel Cyberkriminelle, ist dann im VPN-Tunnel nicht einsehbar, wie die geschützten Daten und Informationen hin und her geschickt werden. Auf VPN setzen daher seit Jahren nicht nur Firmen, sondern auch Behörden.

> Dank des Virtual Private Networks können Mitarbeiter und Unternehmen auf Dateien oder Software sicher zugreifen.

ncp-e.com

Verbindung zwischen Home-Office und Firmennetzwerk

Die aktuelle Herausforderung der IT-Spezialisten: Zum einen ist es nicht banal, das Smartphone oder den Laptop im Wohnzimmer des Mitarbeiters mit dem eigentlich sicher abgeriegelten Netz des Unternehmens zu verbinden. Zum anderen soll diese Verbindung zwischen privatem Netz zu Hause und dem Firmennetzwerk in Zeiten von Corona nun Tausenden gewährt werden.

Verständlicherweise wird es da eng mit VPN-Tunneln: Mit einem Mal braucht es Tausende Lizenzen mehr, wenn der Zugriff dynamisch wächst. Anbieter arbeiten hier mit unterschiedlichen Modellen. Unternehmen können VPN zum Beispiel als Service bei einem Managed Service Provider nutzen oder sich selbst mit der entsprechenden Hardware ausstatten. Hierbei kann es wie zurzeit zu Lieferengpässen kommen, zum Beispiel bei Gateways, Firewalls oder Routern, wenn das Netzwerk schnell in wenigen Stunden oder Tagen ausgebaut werden soll. Andere Anbieter agieren softwarebasiert: VPN-Gateways lassen sich so schneller und einfacher hochfahren. So sind die VPN-Tunnel flexibel erweiterbar. Bezahlt wird die deutlich erhöhte Nutzerzahl z.B. durch „Pay per Use“.

Für einen voll automatisierten Betrieb kommt beim Remote Access ein zentrales Management zum Einsatz: Damit lassen sich die externen Netzwerkzugänge von einer zentralen Stelle aus verwalten, überwachen und Unternehmen haben so ihre VPN Umgebung im Griff. Möglich ist es übrigens, den Remote Access auch für das Industrial Internet of Things zu erweitern. Maschinen sind zwar gegen das Coronavirus immun. Aber noch nicht gegen die Trojaner der Hacker. ■

Dieser Artikel ist in **Zusammenarbeit mit NCP** entstanden.