CASE STUDY

SSP SETZT BEI SECURE REMOTE ACCESS AUF LÖSUNGEN VON NCP

SSP Europe bietet IT-Sicherheit zur Miete an:

Mehr als 800 Kunden und Partner nutzen bereits „Security as a Service", indem sich ihre Mitarbeiter unter anderem über das Produkt SSP Remote Access auf ihr Rechenzentrum einwählen. Technische Basis dafür ist die Remote Access VPN-Lösung von NCP, die SSP auf ihren virtualisierten Rechenzentrums-Ressourcen betreibt.

Von Anfang an: NCP Remote Access VPN

Schon lange bevor es die SSP Europe GmbH gab, hatte ihr Gründerunternehmen, das seit 1993 am Markt etablierte und von Dr. Dieter Steiner gegründete Regensburger Systemhaus A.P.E. GmbH, IT-Sicherheitsdienstleistungen angeboten und ab 2005 das Secure Service Providing (SSP) als Betriebsmodell eingeführt.

Damals hatte sich A.P.E. für die technologisch führende Remote Access VPN Software von NCP entschieden, um ihren Unternehmenskunden sichere Datenverbindungen zu gewährleisten, sei es zwischen deren eigenen Rechenzentren oder angemieteten Ressourcen und vernetzten Standorten, Mitarbeitern in Home Offices oder auch Kunden.
Mit zunehmendem Erfolg des Secure Service Providing wurde SSP im Jahr 2008 als eigenständige GmbH ausgegründet.

Auch die SSP setzte auf die Remote Access VPN Software von NCP. Allerdings bietet sie diese den Kunden und Partnern nun nicht mehr als ausschließlich gekaufte Lizenz, sondern auch als monatliches Mietmodell an.

Überzeugend: Technik und Know-how

„Die Fortsetzung der Zusammenarbeit mit NCP fiel nicht nur aufgrund der bisherigen guten Erfahrungen sehr leicht, sondern hatte auch für die Zukunft sowohl technische als auch strategische Gründe: So überzeugte uns das komplexe Know-how und die Erfahrung von NCP rund um das Thema Remote Access, die umfangreiche Bandbreite an Leistungsmerkmalen wie etwa die End-to-End Sicherheit, das Seamless Roaming und die Skalierbarkeit der Lösung. Dazu kam die regionale Nähe, die immer eine schnelle und erfolgreiche Unterstützung durch den NCP-Support ermöglicht. Beispielsweise, indem NCP auf besondere Wünsche und Feature-Requests unserer Kunden eingeht. Last but not least ist auch das Prädikat ‚Made in Germany' für uns ein positives Marketing-Argument", erklärt Dan Jakob, Head of IT-Security Solutions bei SSP.

Umfangreich: SSP Remote Access über Secure Enterprise Management

Für das Kerngeschäft von SSP ganz besonders wichtig sind das sichere und zentrale Management aller Kundenkonfigurationen auf einer Plattform und die dort abgebildete Multimandantenfähigkeit.

„SSP ist ja nicht ‚ein Kunde', sondern wir nutzen die Infrastruktur für Partner mit jeweils unterschiedlich vielen Kunden und deren Anwendern. Dafür benötigen unsere Administratoren eine übersichtliche und leicht bedienbare Struktur. Auf der anderen Seite müssen die Datenströme der Kunden natürlich voneinander sicher abgeschottet sein. Als wir unser Geschäftsmodell begannen, haben wir das Secure Enterprise Management von NCP, kurz SEM, ausführlich getestet und es hat sich für unsere Zwecke als bestes System im Rahmen eines gemanagten VPN erwiesen", erklärt Jakob.

Das Herz der VPN-Lösung, die SSP unter dem eigenen Produktnamen „SSP Remote Access" vertreibt, ist das zentrale VPN Gateway,

Vorteile für SSP:

- Hochsichere, mandantenfähige IPsec/SSL VPN-Lösung
- Seamless Roaming und „Always on" über alle Verbindungsmedien hinweg
- Einfach bedienbare Administrationsoberfläche für die Benutzerverwaltung
- Preiswertes Mietmodell für Kundenunternehmen
- Ende-zu-Ende-Sicherheit auch an Hotspots
- Kostenüberwachung bei 3G/4G Verbindungen durch Budget Manager

basierend auf dem Secure Enterprise VPN Server (SES) und das Secure Enterprise Management SEM für die Verwaltung und Administration. Auf der zugehörigen SEM-Konsole, einer bedienerfreundlichen Arbeitsoberfläche, werden alle Kunden und deren Nutzer gepflegt. Die Administration ist dabei weitestgehend automatisiert, um manuelle Aufwände in Grenzen zu halten. Baut der Nutzer mit seinem Enterprise Client die Verbindung auf, nimmt der SES die VPN-Anfragen entgegen und ermöglicht den Zugriff auf entsprechende Daten-Ressourcen.

Die NCP-Management Software stellt dafür standardisierte Templates zur Verfügung, die kundenspezifisch angepasst werden können und damit die Grundlage für alle Kunden- und Client-Konfigurationen bilden. Auch die Anlage weiterer Benutzer, zum Beispiel eines neuen Kundenmitarbeiters, gestaltet sich damit sehr einfach. Das betrifft nicht nur die Berechtigungen einzelner User, auf welche Daten sie zugreifen können, sondern auch die Zugriffsart, über welche die Verbindung hergestellt wird und vieles mehr.

Sicher: Authentisierung durch „Besitz und Wissen"

Um die oft sehr sensiblen Firmendaten vor unerlaubtem Zugriff zu schützen, setzt SSP bei der Authentisierung der User auf „Besitz und Wissen": Als „Besitz" wird das individuell auf den Kundenmitarbeiter ausgestellte Benutzerzertifikat bezeichnet, das auf dem Endgerät des Kunden gespeichert ist. Optional kann das Zertifikat auch auf einer, per USB an den Rechner angeschlossenen, Smartcard verwendet werden. Nach der Eingabe der PIN durch den User (Wissen), wird der Verbindungsaufbau initiiert und während der Verhandlung zwischen Client und SES das Zertifikat auf Gültigkeit geprüft und, falls erfolgreich, letztlich der Zugriff gewährt.

„ALS WIR UNSER GESCHÄFTSMODELL BEGANNEN, HABEN WIR DAS SECURE ENTERPRISE MANAGEMENT VON NCP, KURZ SEM, AUSFÜHRLICH GETESTET UND ES HAT SICH FÜR UNSERE ZWECKE ALS BESTES SYSTEM IM RAHMEN EINES GEMANAGTEN VPN ERWIESEN."

Dan Jakob, SSP Europe

Neben Zertifikaten kann der Kunde auch einen One-Time-Password Hardware Token verwenden oder mobile softwarebasierte Token nutzen, welche die OTP-Passwörter auf z.B. einem Smartphone in einer APP generieren. Diese Technologien werden als sogenannte 2-Faktor Authentifizierung bezeichnet.

Einmalig: Seamless Roaming und One Click Solution

Der besondere Charme der VPN-Lösung ist die One Click Solution der IPsec Client Suite, die den Nutzer nach der Authentisierung mit einem einzigen „Klick" auf der grafischen Oberfläche mit dem besten verfügbaren Übertragungsmedium in seine Datenwelt bringt.
Dabei ist es egal, welchen stationären oder mobilen Client er an den verschiedensten Orten nutzt:

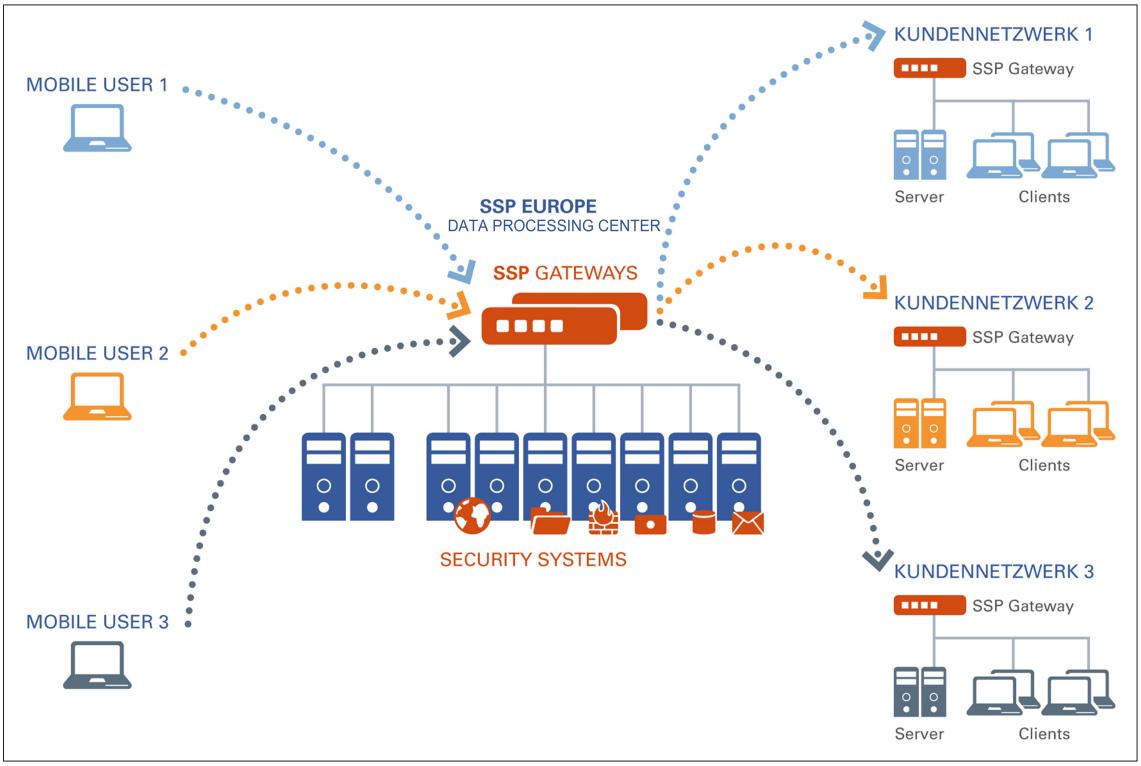

Abb.: Secure Service Providing

Im Büro, an einem vernetzten Standort, im Home Office oder auch am Bahnhof und dann im Zug. Um Seamless Roaming aus verschiedenen Verbindungsarten zu ermöglichen, besitzt die NCP Secure Enterprise Client Suite einen eigenen Dialer mit integrierter 3G/4G-Kartenunterstützung, ein WLAN-Verwaltungstool und eine dynamische Personal Firewall.

Die Client-Software wählt automatisch das passende Firewall-Regelwerk, das optimale Übertragungsmedium, regelt die Einwahl ins Internet und initiiert den Aufbau des VPN-Tunnels. Für den User läuft dies völlig unbemerkt im Hintergrund ab, auch kann er seine Konfigurationsdaten nicht versehentlich ändern, weil dies durch eine zentral vorgegebene Parametersperre verhindert wird.

„SO ÜBERZEUGTE UNS DAS KOMPLEXE KNOW-HOW UND DIE ERFAHRUNG VON NCP RUND UM DAS THEMA REMOTE ACCESS, DIE UMFANGREICHE BANDBREITE AN LEISTUNGSMERKMALEN WIE ETWA DIE END-TO-END SICHERHEIT, DAS SEAMLESS ROAMING UND DIE SKALIERBARKEIT DER LÖSUNG. DAZU KAM DIE REGIONALE NÄHE, DIE IMMER EINE SCHNELLE UND ERFOLGREICHE UNTERSTÜTZUNG DURCH DEN NCP-SUPPORT ERMÖGLICHT. "

Dan Jakob, SSP Europe

„Speziell die Einwahl aus Mobilfunknetzen wird zukünftig immer wichtiger, weil der Einsatz von mobilen Clients, seien es Netbooks, Tablets oder Smartphones auch bei unseren Kunden immer mehr an Bedeutung gewinnt", weiß Dan Jakob.

Preiswert: Security as a Service

SSP bietet sein Remote Access IPsec als SaaS – Security as a Service – für einen geringen monatlichen Betrag monatlich pro Client inklusive Wartung an. Dabei ist es unerheblich, ob die Kunden ein eigenes Rechenzentrum oder die SSP-Ressourcen in Deutschland und seit 2012 auch in Österreich nutzen, wie viele Clients durch Unternehmenswachstum hinzukommen oder auch gekündigt werden. Der Vorteil für den Kunden liegt auf der Hand: Er hat keine Investitionskosten für eigene Server und Software sowie Personal für die Einrichtung und Verwaltung, zudem ist die Lösung beliebig skalierbar. „Wir haben aber auch Kunden, die eigene Lizenzen auf eigenen Servern haben, in diesem Fall betreiben wir die SSP Remote Access Lösung für den Kunden, so dass er seine sicheren Verbindungen immer in kompetenter Hand und auf dem neuesten Stand weiß.

Über SSP Europe

SSP Europe ist ein Secure Service Provider mit Hauptsitz in München. Das 2008 gegründete Unternehmen bietet „Security-as-a-Service" für rund 800 Unternehmen jeder Größenordnung, u.a. McDonald´s oder den Sportartikelhersteller Völkl. Zum Angebot gehören Sicherheits-Services, vom All-inklusive-Firewall-Dienst, über Spam-Abwehr und Virenschutz bis hin zu Exchange-Services oder auch Online-Backup. Eigenentwicklungen wie der SSP Secure Data Space (eine sichere Dateiaustauschplattform für Unternehmen) oder das SSP Control Board (eine zentrale Plattform für Logauswertungen, Compliance-Berichte und Konfiguration von IT-Services) runden das Portfolio ab. SSP Europe beschäftigt derzeit mehr als 50 Mitarbeiter und bietet seine Leistungen und „Security as a Service" über ein dynamisches Partnermodell durch Systemhäuser, VARs, Softwareanbieter und Provider bzw. Vermittlungspartner an.

Dan Jakob, Head of IT-Security Solutions SSP Europe GmbH

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.

NCP SECURE COMMUNICATIONS

NCP engineering GmbH
Dombühler Str. 2
90449 Nürnberg

Telefon: +49 911 9968 0
Fax: +49 911 9968 299
E-Mail: info@ncp-e.com

www.ncp-e.com