CASE STUDY

SICHERHEIT IM WLAN FÜR SENSIBLE DATEN

Unzureichende Sicherheit im Wireless LAN (WLAN) und ein eingeschränktes Management der mobilen Endgeräte gehörten zu den Gründen, weshalb sich das Schweizer Versicherungsunternehmen Die Mobiliar dafür entschieden hat, ihre bisherige Virtual Private Network (VPN)-Lösung zu ersetzen. Mit der neuen, vollautomatisierten Remote Access VPN-Lösung von NCP erwarten die Verantwortlichen der Mobiliar eine verbesserte Effizienz der Kommunikationsprozesse sowie ein höhere Produktivität der Mitarbeiter.

Um im heutigen Wettbewerb ganz vorne dabei zu sein, ist es wichtig, dass Unternehmen flexibel agieren und kurzfristig auf Marktanforderungen reagieren können. Auch die Mobiliar, die älteste private Versicherungsgesellschaft der Schweiz, stellte die Weichen für eine mobile Datenkommunikation auf Basis modernster Remote Access-Technologie. Denn eine der Stärken der Mobiliar ist ihre dezentrale Struktur: Über 80 Unternehmer-Generalagenturen mit rund 60 angegliederten Agenturen garantieren Kundennähe und lokale Kompetenz in der ganzen Schweiz.

Bereits 2001 installierte die Mobiliar ein Virtual Private Network auf Basis des IPsec-Standards zur Anbindung der Generalagenturen und Agenturen, der Außendienstmitarbeiter sowie der Mitarbeiter an den Direktionsstandorten in Bern und Nyon. Der Zugriff auf versicherungsspezifische Applikationen, Host-Systeme, Microsoft Outlook und auf das Intranet erfolgte allerdings ausschließlich über eine LAN-Schnittstelle (Local Area Network), was die Möglichkeiten für Remote Access einschränkte.

Aufgrund gestiegener Mobilitätsanforderungen war die Nutzung von WLAN-Netzwerken unumgänglich. Die Geschäftsleitung forderte, dass sich Mobiliar Mitarbeiter von überall her mit dem Firmennetzwerk verbinden können - auch an öffentlichen WLAN Hotspots. Die strikte Vorgabe dabei war, dass die gesamte Datenkommunikation ausschließlich über das Mobiliar Netzwerk abläuft. Es sollte kein Bit am Server der Mobiliar vorbeigehen, was bei der Hotspot-Anmeldung problematisch ist, da die Registrierung außerhalb des geschützten Bereichs eines VPN mittels Web-Browser erfolgt. Diese Schwachstelle galt es zu umschiffen.

„Öffentliche WLAN-Netze sind wesentlich schwieriger zu sichern als ein LAN. Trotzdem gilt es hier, denselben Sicherheitslevel zu gewährleisten. Deshalb muss verhindert werden, dass Benutzer unkontrollierten Zugang ins Internet haben und sich dabei Schadsoftware auf das Gerät laden. Gleich konsequent muss auch das Endgerät – Laptop, Notebook, Smartphone etc. - vor unerwünschten Zugriffen anderer Hotspot-Teilnehmer oder Angreifer geschützt sein“, erklärt Stefan Geiser, verantwortlich für die Einführung der neuen VPN-Lösung bei der Mobiliar.

Komplexe Sicherheitsanforderungen

Eine wichtige Anforderung war daher eine „Location Awareness“-Funktion der Firewall. Der Grund:

Projektanforderungen:

- Benutzer sollen sich von überall her mit der Mobiliar verbinden können
- WLAN-Netzwerke sollen ausdrücklich verwendet werden können, insbesondere PWLAN Hotspots
- Benutzer dürfen keinen unkontrollierten Zugang ins Internet haben
- Gerät muss in jedem Fall vor unerwünschten Zugriffen geschützt sein
- Location Awareness
- Unterstützung der Smartcard-Funktionalität
- Bessere Verwaltbarkeit
- Lösung muss einfach bedienbar sein, auch scriptfähig
- Verwendung von Zertifikaten, welche sich im lokalen Benutzerzertifikatsspeicher befinden (CSP)

Beim Einwählen in ein öffentliches Netzwerk konnte nicht ausgeschlossen werden, dass dieses im gleichen Addressbereich lag wie das interne Mobiliar Netzwerk.

Ohne Location Awareness wären die Geräte netzwerkseitig ungeschützt offen gestanden. Dies musste bei der Freischaltung von WLAN verhindert werden.

„UNSERE VORSTELLUNG WAR, DASS WIR ÜBER EIN ZENTRALES REMOTE ACCESS MANAGEMENT ALLES DEFINIEREN KÖNNEN, WAS AUF DIE CLIENTS AUSWIRKUNGEN HAT."

Stefan Geiser, Die Mobilar

Ein weiterer Knackpunkt war, dass die Anmeldung an bestimmten öffentlichen WLAN Hotspots in der Schweiz SMS-basiert erfolgt. Der Benutzer registriert sich auf der Website des Hotspot-Betreibers, indem er die Rufnummer seiner Datenkarte eingibt. Anschließend wird ihm für die Registrierung eine SMS mit einer PIN zugesendet.

Und es galt noch eine Mobiliar spezifische Anforderung zu erfüllen: Die Authentisierung der VPN-Verbindung sollte über den Zertifikatsspeicher von Microsoft erfolgen. Die Client Software musste also die CSP (Cryptographic Service Provider)-Anbindung unterstützen.

Trotz aller komplexen Sicherheitsanforderungen sollte die Software für den Anwender leicht bedienbar sein. Die Anforderungen waren auch hier klar definiert: Die Einwahl ins Internet und der Aufbau des VPN-Tunnels sollten künftig über ein einziges Tool gesteuert werden. Bislang wurde die UMTS-Verbindung im Hintergrund über ein Script gestartet. Anschließend erfolgte eine Überprüfung der Verbindung, dann wurde über den VPN Client der IPsec-Tunnel aufgebaut. Dabei musste jedes Mal geprüft werden, ob eine Verbindung ins Internet bestand oder nicht.

Auch das Management der VPN Clients galt es zu optimieren. Das Manko der bisherigen Lösung war, dass die Sicherheitspolicies für Clients nur dann aktualisiert werden konnten, wenn die Endgeräte per VPN mit dem Server verbunden waren. Da es aber Benutzer gab, die sich nicht regelmäßig ins Netzwerk einwählten, gab es Einschränkungen bei der Aktivierung neuer Firewall-Regeln. „Unsere Vorstellung war, dass wir über ein zentrales Remote Access Management alles definieren können, was auf die Clients Auswirkungen hat, und dass diese Änderungen in kürzester Zeit automatisiert weitergeleitet werden", so Geiser.

Last but not least gab es noch eine Voraussetzung: Die VPN Client Software musste kompatibel sein zur bereits im Einsatz befindlichen Lösung zur Datenoptimierung von Riverbed.

Kurze Pilotphase

Vor dem Hintergrund dieses Anforderungskatalogs stieß die bisher eingesetzte VPN-Lösung von Checkpoint an ihre Grenzen. Infolgedessen testeten Geiser und sein Projekt-Team die VPN-Lösungen verschiedener Hersteller. Doch keine der Lösungen konnte alle Kriterien erfüllen - insbesondere was die Sicherheitsanforderungen für WLAN betraf. Die IT der Mobiliar stand unter enormem Zeitdruck, als sie im Zuge der Evaluierung im Oktober 2009 auf die VPN-Lösung der Nürnberger NCP engineering GmbH stieß. Die Lösung versprach nicht nur, der drängensten Forderung nach Location Awareness schnell gerecht zu werden, sie bot darüber hinaus ein zentrales Remote Access Management und einen „One Click" VPN Client mit essentiellen Funktionen.

Nach einer kurzen Pilotphase, während der NCP zusätzlich die Microsoft CSP-Anbindung und die SMS-Funktion in seinen VPN Client integrierte, erhielten die Nürnberger Anfang Dezember 2009 den Zuschlag. „Dank der intensiven Zusammenarbeit mit der Entwicklungsabteilung und einem hervorragenden Support durch die NCP System Engineers vor Ort konnten wir innerhalb von fünf Wochen die Lösung zum Laufen bringen. NCP hat sehr dynamisch und flexibel reagiert und die Lösung optimal auf unsere Bedürfnisse abgestimmt", erläutert Geiser.

Zentrales Management

Die neue Remote Access-Lösung der Mobiliar ist zentral administrierbar und basiert auf NCPs „Next Generation Network Access Technology" - einer ganzheitlichen, softwarebasierten Remote Access-Lösung. Es wurden vier Komponenten implementiert: die Secure Enterprise Client Suite, der Secure Enterprise VPN Server, der Secure Enterprise Failsafe Server und das Secure Enterprise

Management. Alle Komponenten ließen sich nahtlos in die vorhandene Netzinfrastruktur integrieren. Die Aktualisierung der VPN Clients erfolgt über die Update-Funktion des

NCP Secure Enterprise Management (SEM). Diese Funktion führte zu einer erheblichen Arbeitserleichterung der Administratoren und war entscheidend bei der Implementierung der Lösung. „Die Umsetzung unseres Projektes wäre sonst in dieser Form nicht möglich gewesen, denn die Update-Funktion des SEM ist einfacher zu handhaben als die komplexen Mechanismen einer herkömmlichen Softwareverteilung. Alle Software und Konfigurations-Updates, die Verwaltung von Usern, Lizenzen und Zertifikaten erfolgen automatisiert über eine einzige Konsole. Wir haben die Möglichkeit, Policy-Änderungen ganz flexibel und innerhalb von nur 15 Minuten durchzuführen", erklärt Geiser.

Alle Statusinformationen werden den IT-Administratoren bei der Mobiliar übersichtlich und in Echtzeit am Systemmonitor zur Verfügung gestellt. Innerhalb des SEM erfolgt auch die komplette Benutzerverwaltung. Das VPN Management System führt in regelmäßigen Zeitabständen eine automatische Synchronisation mit dem Active Directory durch. Alle Clients können dennoch bei Bedarf individuell verwaltet und konfiguriert werden. Der Verwaltungsaufwand für die IT-Mitarbeiter ist dabei sehr gering.

„One Click" Solution

Insgesamt sind 2.500 Benutzer in das VPN eingebunden. Sie können sich auf einfache Weise und vor allem sicher auch per UMTS von jedem beliebigen Standort in das Firmennetz einwählen.

Im Gegensatz zu herkömmlichen VPN Clients verfügt die NCP Secure Enterprise Client Suite über einen eigenen 3G Dialer mit integrierter UMTS-Kartenunterstützung, ein WLAN-Verwaltungstool und eine Personal Firewall. Der Benutzer arbeitet dabei nur mit einer grafischen, intuitiven Oberfläche. Sämtliche Module sind von der IT zentral administrierbar. Aus Sicherheitsgründen und um den Benutzern die Bedienung so einfach wie möglich zu gestalten, übernimmt der VPN Client als „One Click" Solution nach Klicken auf „Verbindung" automatisch alle weiteren Aktivitäten: Die Auswahl des Übertragungsnetzes und die Einwahl ins Internet, den Aufbau des VPN-Tunnels zur Firmenzentrale sowie die Auswahl des richtigen Firewall-Regelwerks. Zudem wurde der Client so konfiguriert, dass bei erfolgter VPN-Verbindung automatisch die benutzerspezifischen Laufwerkszuordnungen zum zentralen File Server erfolgen.

Location Awareness

Der NCP Client unterscheidet drei Zonen: unbekannte (unsichere) Netze, VPN-Zugriff und bekannte (sichere) Netze. Ist der Anwender beispielsweise über seinen Rechner mit dem Firmen-LAN verbunden und hat parallel noch eine Verbindung mit einem WLAN-Adapter zum Hotspot, erkennt die Software automatisch, welche Netzwerkverbindung „sicher" und welche „unsicher" ist. Die integrierte Firewall schirmt den Rechner sofort über ein spezielles Regelwerk ab, welches von der Mobiliar zentral vorgegeben und vom Anwender nicht veränderbar ist. Somit kann eine WLAN-Verbindung auch dann gefahrlos aktiv bleiben, wenn sich der Benutzer im Intranet befindet.
Für eine sichere Einwahl am Hotspot (Hotspot Login-Funktion) stellt die Personal Firewall in Abhängigkeit vom Verbindungsstatus sicher, dass nur die Hotspot-Anmeldung und der VPN-Aufbau erfolgen, jedoch keine weiteren Programme „direkt" auf das Internet zugreifen können.
Alle Firewall-Mechanismen sind bereits beim Systemstart aktiviert und bleiben auch aktiv, wenn kein VPN-Dienst genutzt wird. Des Weiteren lässt sich der Client so konfigurieren, dass er auch aus Netzen heraus IPsec-Tunnel aufbauen kann, in denen die üblichen VPN-Ports gesperrt sind (NCP Path Finder Technology).

Um eine hohe Verfügbarkeit des NCP Secure Enterprise VPN Servers im Rechenzentrum sicherzustellen, wurde das System redundant ausgelegt und durch einen NCP Secure Enterprise Failsafe Server erweitert.

Hohe Benutzerakzeptanz

Der Wechsel auf die Next Generation Network Access Technology von NCP hat sich für die Mobiliar gerechnet: Durch das zentrale Monitoring und Management verbucht die IT der Mobiliar einen Effizienz-Gewinn. Die Mitarbeiter haben

**„ES GIBT NUR NOCH EINE SOFTWARE, DIE ALLES STEUERT.
DIE MITARBEITER SCHÄTZEN ES, SICH – EGAL WO SIE SIND - EINFACH MIT EINEM KLICK EINWÄHLEN ZU KÖNNEN. "**

**Stefan Geiser,
Die Mobilar**

über WLAN sicheren Zugriff auf das Firmennetzwerk und können genauso wie im Büro arbeiten. „Es gibt nur noch eine Software, die alles steuert. Daher haben wir auch eine hohe Benutzerakzeptanz. Die Mitarbeiter schätzen es, sich – egal wo sie sind

- einfach mit einem Klick einwählen zu können. Entsprechend gering ist auch die Anzahl der Trouble Tickets und unser Supportaufwand", resümiert Geiser.

„NCP HAT SEHR DYNAMISCH UND FLEXIBEL REAGIERT UND DIE LÖSUNG OPTIMAL AUF UNSERE BEDÜRFNISSE ABGESTIMMT"

Stefan Geiser, Die Mobiliar

Für die Zukunft plant die Mobiliar, die NCP Remote Access-Lösung auf die für 2012 geplante neue Geräteplattform zu portieren. Ziel ist es, verstärkt von den flexiblen Nutzungsmöglichkeiten moderner Kommunikationsmedien zu profitieren – und das auf weiterhin hohem Sicherheitsniveau.

Die Mobiliar

Jeder dritte Haushalt in der Schweiz ist bei der Mobiliar versichert. Der Allbranchenversicherer weist ein Prämienvolumen von 2,9 Mia. Franken auf. Über 80 Unternehmer-Generalagenturen mit eigenem Schadendienst garantieren Nähe zu den 1,5 Millionen Kunden. Die Schweizerische Mobiliar Versicherungsgesellschaft AG ist in Bern, die Schweizerische Mobiliar Lebensversicherungs-Gesellschaft AG in Nyon domiziliert. Zur Gruppe gehören ferner die Protekta Rechtsschutz-Versicherung AG, die Protekta Risiko-Beratungs-AG, die Mobi24 Call-Service-Center AG und die XpertCenter AG, alle mit Sitz in Bern.

Die Mobiliar beschäftigt in den Heimmärkten Schweiz und Fürstentum Liechtenstein 3603 Mitarbeitende (Vollzeitstellen) und bildet zurzeit 300 Lernende aus. Sie ist die älteste private Versicherungsgesellschaft des Landes und seit ihrer Gründung 1826 genossenschaftlich verankert.

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.

„Der Wechsel hat sich für uns gelohnt!"

Stefan Geiser, verantwortlich für die Einführung der neuen VPN-Lösung bei dem Schweizer Versicherungsunternehmen Die Mobiliar

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