LANCOM Whitepaper

Home-Office – Sicheres Arbeiten von zu Hause

Digitale Technologien legen die Basis für mehr Flexibilität in der heutigen Arbeitswelt und erleichtern die Lebenssituationen vieler Arbeitnehmer: Die Vereinbarkeit von Familie und Beruf, unnötige Fahrten für Präsenzmeetings, die Verantwortung für entlegene Vertriebsgebiete, die Arbeit als Handelsvertreter für ausländische Unternehmen – alles Themen, auf welche die Bereitstellung von Heimarbeitsplätzen eine Antwort gibt. Auch in außergewöhnlichen Situationen wie z. B. Extremwetter, Quarantänesituationen oder Hochwasser bleibt ein Unternehmen, welches seinen Mitarbeitern Home-Office ermöglicht, geschäftsfähig – ganz im Sinne des Business Continuity Managements. Allerdings haben weiterhin viele Unternehmen Bedenken bei der Umsetzung von Telearbeit, unter anderem aus Sicherheits- und Kostengründen. In diesem Whitepaper werden Lösungen zur Umsetzung einer modernen, sicheren und kosteneffizienten VPN-Infrastruktur vorgestellt.

VPN – die Verlängerung des Firmennetzes nach Hause

„My home is my office" ist kein Wunschtraum, sondern mit heutigen Netzwerklösungen einfach und günstig realisierbar. Standortvernetzung heißt das Stichwort, die vollständige Integration von Telearbeitsplätzen in das Netzwerk des Unternehmens. Der Charme einer solchen Lösung: die Arbeitnehmer arbeiten von daheim ganz so, als wären sie im Büro – und greifen wie selbstverständlich auf E-Mail, Netzwerk, Server, Telefon und digitale Dienste zu. Auch die Konfiguration der Geräte im Home-Office erfolgt aus der Ferne über die zentrale IT-Abteilung. Als günstiges Vernetzungsmedium dient die Standard-Internetleitung

über DSL, Kabel oder Mobilfunk, die heute quasi jeder Haushalt hat. Die Verbindung wird dabei durch ein Virtual Private Network (VPN) vollständig abgesichert.

Genauso, wie die Standorte eines Unternehmens miteinander vernetzt werden, können auch mobile Mitarbeiter sowie Heimarbeitsplätze schnell und vor allem sicher über ein VPN ins Unternehmensnetz eingebunden werden. Einzige Voraussetzung ist ein kleines Software-Tool: ein VPN-Client auf dem Laptop oder PC. Ist der VPN-Zugang einmal konfiguriert, wird mit nur einem Klick die hochverschlüsselte VPN-Verbindung über das beste verfügbare Verbindungsmedium aufgebaut. Auch über mobile Endgeräte wie Smartphones oder Tablet-PCs kann sicher über VPN mit der Firma kommuniziert werden. Hierbei wird mithilfe einer App eine sichere VPN-Verbindung zum zentralen Unternehmens-Gateway eingerichtet.

Home-Office auch in Deutschland auf dem Vormarsch

Die Unternehmen haben die Chancen der Telearbeit erkannt. Nutzten 2014 nur rund 20 % die Möglichkeit, Mitarbeiter im Home-Office arbeiten zu lassen, hat sich

der Anteil in nur vier Jahren fast verdoppelt: Im Jahr 2018 ließen bereits 39 % der Unternehmen ihre Mitarbeiter auch von zu Hause aus arbeiten, berichtet der Digitalverband Bitkom[1]. 46 % der Befragten denken außerdem, dass sich die Telearbeit in den nächsten fünf Jahren immer mehr durchsetzen wird; ganze 50 % erwarten hier jedoch keine Steigerung.

Unternehmen, die sich gegen Home-Office entscheiden, geben häufig innerbetriebliche Bedenken an – Bedenken, die sich durch klare Regelungen zur Home-Office-Nutzung häufig lösen lassen würden. Gleichzeitig werden Bedenken in den Bereichen Datensicherheit (22 %) und Kosten zur Ausstattung von Heimarbeitsplätzen (12 %) angegeben. Und das obwohl moderne VPN-Lösungen sicher verschlüsselt und zugleich sehr kostengünstig sind.

Die Lösung für das sichere Home-Office – LANCOM Advanced VPN Client

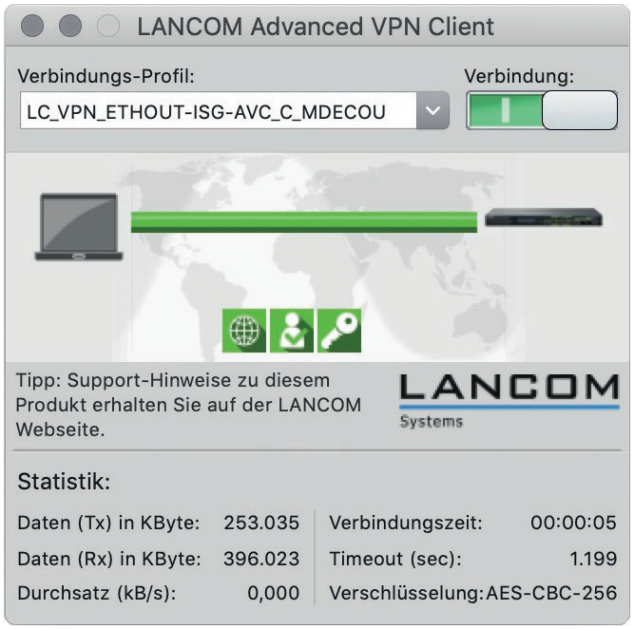
Mit dem LANCOM Advanced VPN Client für die Betriebssysteme Windows und macOS kann der Nutzer über einen gesicherten VPN-Tunnel mit nur einem Klick auf das Unternehmensnetzwerk zugreifen. Hierbei spielt es keine Rolle, ob sich der Anwender im Home-Office, im Ausland oder in einem Verkehrsmittel befindet. Ausgerüstet mit einer Stateful Inspection Firewall erkennt der Software-VPN-Client automatisch sichere und unsichere Netze für eine jederzeit abgesicherte Kommunikation über das Internet.

Für den Aufbau des VPN-Tunnels kommen state-of-the-art Verschlüsselungstechnologien wie das moderne und effiziente VPN-Protokoll IKEv2 zum Einsatz. Zusätzlich unterstützt der LANCOM Advanced VPN Client moderne Verschlüsslungsalgorithmen wie AES-CBC oder AES-GCM, die Signaturfunktionen SHA-256, SHA-384 oder SHA-512 sowie aktuelle Diffie-Hellmann Gruppen.

Die VPN-Aushandlung zwischen dem VPN-Gateway im Unternehmen und dem Software-VPN-Client erfolgt über verschiedene Wege – je nach Unternehmensgröße und Anforderung:

- Für kleinere bis mittlere Unternehmen: sehr einfach einzurichten und zu bedienen über Eingabe eines Passworts (Authentifizierung über Pre-Shared Key – PSK)
- Für größere Szenarien mit erhöhtem Sicherheitsbedarf: Der Einsatz von IKEv2 mit digitalen Zertifikaten
- Für große Szenarien mit Windows-Server-Infrastruktur: IKEv2 EAP für eine Authentifizierung über den Windows-Server mit Benutzername und Passwort
- Für große Szenarien mit zentraler Benutzerverwaltung: direkte und aufwandsarme Authentifizierung über einen RADIUS-Server

Für einen reibungslosen Arbeitsablauf werden sowohl IPv4- als auch die steigende Anzahl an IPv6-Anschlüssen unterstützt. Und dank Seamless Roaming-Funktionalität bleiben auch bei Medienwechseln VPN-Verbindungen bestehen. So bleibt die VPN-Verbindung beispielsweise auch bei Bahnfahrten beim Wechsel zwischen Mobilfunkzellen durchgängig aufrechterhalten. Ebenso hat der Benutzer in Gebäuden beim Roaming von Mobilfunk zu WLAN oder Ethernet ein „always on"-Erlebnis.



1 https://www.bitkom.org/Presse/Presseinformation/Vier-von-zehn-Unternehmen-setzen-auf-Homeoffice

Da insbesondere in Hotels oder öffentlichen Hotspots eine Firewall häufig IPSec-Kommunikation blockt (Port 500, 4500), wird über die Technologie IPSec-over-HTTPS (basierend auf der NCP VPN Path Finder Technology) ein Verbindungsaufbau initiiert, bei dem das IPSec-VPN mit einem zusätzlichen SSL-Header (Port 443, wie bei HTTPS) gekapselt wird.

Zudem kann zur Entlastung des Firmennetzwerks z. B. Internetverkehr direkt ins Internet geleitet werden, sofern sich der Mitarbeiter in einem vertrauenswürdigen Netzwerk befindet. Daten für das Firmennetzwerk hingegen werden weiterhin über den VPN-Tunnel geleitet (Split-Tunneling). Befindet sich der Mitarbeiter hingegen in einem unverschlüsselten, also unsicheren WLAN, werden alle Daten sicher vom VPN-Tunnel verschlüsselt an die Zentrale übertragen, wo diese dann sicher ins Internet geleitet werden (Full-Tunneling).

Trotz des großen Funktionsumfangs geht die Konfiguration des LANCOM Advanced VPN Clients auf den Mitarbeiter-Laptops leicht von der Hand: VPN-Zugänge zur Unternehmenszentrale lassen sich sehr einfach mit einem „1-Click-Setup-Assistenten" erstellen und in eine Datei exportieren, die vom VPN-Client als Profil eingelesen werden kann. Dabei werden die erforderlichen Informationen der aktuellen Konfiguration der VPN-Gegenstelle in der Unternehmenszentrale entnommen und mit zufällig ermittelten Werten ergänzt (z. B. für den Preshared Key). Somit lassen sich in kürzester Zeit mehrere VPN-Zugänge für Mitarbeiter erstellen und einrichten - eine echte Zeitersparnis für den Administrator.

Eine Sammlung an vielen hilfreichen Konfigurationsanleitungen finden Sie in der LANCOM Knowledge Base.

Eine Rechnung, die aufgeht

Die Investition in eine passende Sicherheitsinfrastruktur für mobiles Arbeiten ist überschaubar. Auf der Unternehmensseite wird ein einziges Gerät benötigt, nämlich ein VPN-fähiger Router, ein zentrales VPN-Gateway oder eine VPN-fähige Firewall. Für die Ausstattung der Mitarbeiter-Laptops genügt der kostengünstige LANCOM Advanced VPN Client – der zudem mit Produkten vieler Hersteller kompatibel ist.

Diese Investition rechnet sich – und zwar auf beiden Seiten.

Bei Telearbeit profitieren Mitarbeiter vom Wegfall der An- und Abfahrtswege, sparen Zeit und Benzinkosten. Die Firmen erhöhen die Produktivität ihrer Mitarbeiter, benötigen gegebenenfalls sogar weniger Bürofläche, sparen Miete und senken ihre laufenden Betriebskosten. Und: Sie können sich flexibel und familienfreundlich positionieren und so im harten Wettbewerb um Fach- und Führungskräfte innovativ punkten.

Fazit

Unsere Welt verändert sich – und Mobilität wird eine Grundvoraussetzung für viele Unternehmen und ihre Mitarbeiter. Mit einem VPN-Client können sich die Mitarbeiter mit ihrem Laptop über das Internet von überall sicher in das Unternehmensnetzwerk einloggen und auf interne Daten zugreifen. Das ermöglicht ihnen maximale Flexibilität, egal ob sie sich auf Geschäftsreise befinden oder von zu Hause aus arbeiten möchten. Sicherheits- und Kostengründe werden zwar häufig als Grund gegen den Einsatz von Home-Office im eigenen Unternehmen genannt, werden jedoch mit einer zeitgemäßen und effizienten VPN-Gesamtlösung von LANCOM in Einsparpotentiale umgemünzt.

Frequently Asked Questions (FAQ)

Kann ich meinen LANCOM Router um zusätzliche VPN-Verbindungen erweitern?

Mit der LANCOM VPN Option lässt sich die Anzahl der VPN-Kanäle je nach LANCOM Gerät erweitern. So können beispielsweise alle LANCOM Router der 17xx-Serie im Auslieferungszustand bis zu 5 VPN-Tunnel aufbauen und können darüberhinaus auf bis zu 25 Tunnel erweitert werden. Siehe auch: https://www.lancom-systems.de/produkte/software-optionen/lancom-vpn-option/.

Kann ich mein VPN-Profil in mehrere Endgeräten importieren und gleichzeitig anwenden?

VPN-Benutzerprofile können grundsätzlich in mehrere VPN-Client-Installationen (z. B. unterschiedliche Rechner) importiert werden. Allerdings ist pro VPN-Profil nur eine Sitzung gleichzeitig möglich.

Wo kann ich nachvollziehen, wie viele VPN-Verbindungen aktiv sind?

Aktive VPN-Client-Verbindungen können übersichtlich über LANmonitor eingesehen werden.

Kann ich als Administrator VPN-Verbindungen zentral deaktivieren?

Ausgewählte VPN-Einwahlverbindungen können bei Bedarf über LANconfig bzw. WEBconfig deaktiviert werden.

Welchen Funktionsumfang bietet der LANCOM Advanced VPN Client in der Demo-Version?

Der LANCOM Advanced VPN Client bietet eine kostenlose 30-Tage-Demo-Version im vollen Funktionsumfang. Bitte beachten: Es können maximal drei VPN-Verbindungen im unlizenzierten Zustand zur VPN-Gegenstelle aufgebaut werden.

Kann ich den LANCOM Advanced VPN Client auch in Kombination mit LANCOM R&S®Unified Firewalls anwenden?

Ja. Mit dem aktuellen Betriebssystem LCOS FX 10.4 bieten LANCOM R&S®Unified Firewalls die Möglichkeit, Import-Profile für den LANCOM Advanced VPN Client einzurichten.