Home Office

Veröffentlicht: Montag, 11. Jan 2021

Am 8.1.2021 erschien eine Sonderseite in der Verdener Aller Zeitung zum Thema Home Office - Schubert IT war selbstverständlich auch dabei!

Hier unser Anteil oder die ganze Seite als PDF zum Download:

Aufgrund der Corona Pandemie haben die Begriffe Home-Office, Firewall und VPN eine neue Berühmtheit erlangt. Niemand, der nicht berufsmäßig mit ITBetreuung zu tun hatte, oder viel im Außendienst unterwegs war, hat sich damit vorher beschäftigt. Im Zuge des Infektionsschutzes wurden schlagartig hunderttausende Arbeitsplätze in das private Umfeld der Mitarbeiter verlagert.

Internet hat jeder – aber die wenigstens Menschen haben ein professionell administriertes und gemanagtes Netzwerk zu Hause. So musste sich umgehend über Fernzugänge, Sicherheitsregeln und Bandbreiten Gedanken gemacht werden. Laut den Experten von Schubert IT gibt es drei große Themenbereiche im Home-Office zu beachten, die sie im Folgenden erklären: Die Bandbreite der Internetzugänge: Generell kann man sagen, dass es nie genug Bandbreite sein kann. Um ein Home-Office, also ein vollwertiges Büro im Wohn- oder Esszimmer zu installieren, raten die Experten zu einem Internetzugang mit einer Bandbreite ab circa 50 Mbit/s Downstream (= Geschwindigkeit der Daten aus dem Internet zum PC oder Notebook). In Deutschland sind sogenannte „asynchrone“ Verbindungen der Standard. Dies bedeutet eine „50000er“-Leitung, also 50 Mbit/s Downstream. Diese stellt nur sehr selten diese Bandbreite auch in die andere Richtung (Upstream =Weg der Daten vom PC oder Notebook ins Internet) zur Verfügung. Wird also etwas aus dem Internet heruntergeladen, geht dies meist vier- bis achtmal

so schnell wie der Weg von PC oder Notebook ins Internet beziehungsweise zum Unternehmen. Für die Heimanwendung wie Streaming, Updates oder schlichtes „surfen“ ist das absolut ausreichend – produktive Arbeit setzt jedoch eine zuverlässige Verbindung in beide Richtungen voraus. Erschwerend müssen parallel oft Daten für die Telefonie (VoIP) noch über die gleiche Leitung geschickt werden. Alles in allem „ein Kraftakt für den Internetzugang“.

Zusätzlich zur Bandbreite im Home-Office muss auch im Unternehmen genügend davon vorhanden sein. Alles, was vorher über das lokale Netzwerk im Unternehmen aus den Büros auf den Servern gearbeitet wurde, muss nun durch den „Flaschenhals namens Internetanschluss“ zu den Mitarbeitern ins Home-Office. Hier kommen auch schnelle Anschlüsse oft an ihre Grenzen – sofern diese überhaupt verfügbar sind. Die Alternative ist der Betrieb von Servern in einem externen Rechenzentrum. Bei dieser Lösung werden einzelne Teile der IT oder die ganze Infrastruktur ausgelagert und alle Mitarbeiter verbinden sich dorthin. Die Rechenzentrums-Anbieter verfügen meist über deutlich höhere Bandbreiten.

Firewall: Wenn die Bandbreite ausreicht, wird oft ein weiterer Aspekt vergessen: der Weg der Daten rein und vor allem raus aus dem Netz des Unternehmens. Es ist dafür zu sorgen, dass über das Internet übertragene Daten nicht von anderen, betriebsfremden Personen abgefangen werden können. Auf der Seite des Unternehmens sollte auf jeden Fall eine Firewall mit aktuellen Viren-Informationen sowie sauber konfigurierten Zugriffs-Regeln vorhanden sein.

Eine Firewall ist ein System, das zwischen dem Router des Internetzugangs (zum Beispiel FritzBox) und dem Netzwerk des Unternehmens geschaltet wird. Diese Firewall untersucht und erlaubt den Datenverkehr zwischen den Servern, Endgeräten und dem Internet. Um aus dem Home-Office auf die Daten im Unternehmen zugreifen zu können, sollte dort ebenfalls eine Firewall hinter dem Router des privaten Internetzugangs (zum Beispiel FritzBox) geschaltet sein. Diese Firewall baut dann eine sogenannte VPN-Verbindung (VPN = Virtual Privat Network) zum Firmennetz auf. So entsteht eine direkte, verschlüsselte Verbindung aus dem privaten Bereich zum Unternehmen. Es können mehrere Geräte (PC, Notebook, Drucker, Telefon, etc.) aus dem Home-Office mit dem Firmennetz verbunden werden. Vorzugsweise per Kabel oder zur Not per WLAN. Bei der Verwendung von WLAN sind die Vorgaben des
Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Verschlüsselung zu beachten: www.bsi-fuer-buerger.de.

Sollte der Aufwand einer zusätzlichen Firewall im Privathaus der Mitarbeiter den Rahmen sprengen oder nur temporär auf einem Endgerät ein Zugang benötig werden, dann kann eine VPN-Verbindung auch direkt vom Endgerät aus aufgebaut werden. So entfällt die Installation einer Firewall und auf dem Endgerät wird lediglich ein „VPN Client“ installiert. Dieser erstellt dann die verschlüsselte Verbindung zur Firewall im Unternehmen.

Virenschutz: Da jedes Endgerät im Home-Office mit dem Internet verbunden ist, ist ein Virenschutz unerlässlich. Der PC oder Laptop wird nicht sofort „krank“, wenn kein solcher Schutz vorhanden ist, aber es ist wahrscheinlicher, dass es zu unerwünschter Installation von Software auf dem Endgerät kommt. Solche Software kann zum Beispiel dafür sorgen, dass eine VPNVerbindung nicht mehr so sicher ist, wie sie sein sollte oder Inhalte von Mails sowie Zugangsdaten für Portale bis hin zum Banking „abgefischt“ werden können. Grundsätzlich gilt auch ohne Home-Office und sensible Daten: Jeder PC oder Laptop sollte über einen solchen Schutz verfügen (siehe auch hier die Vorschläge des BSI).

Schreiben Sie uns gerne Kontakt mit uns auf!

Zurück