Foto: ©tippapatt/stock.adobe.com, cimdata software GmbH

Digitalisierung im Home-Office

Sicheres Arbeiten

Nicht nur bei uns heißt es nun: „Öfter von zu Hause aus arbeiten". Aber wie funktioniert das am besten – und vor allem auch sicher?

IN VIELEN Firmen ist „Work from home" durch die Corona-Pandemie ein sehr wichtiges Thema geworden. Die Mitarbeiter, bei denen es ohne Probleme technisch möglich ist, arbeiten von zu Hause aus. Manche stehen vielleicht wegen Kontakt zu einer auf Covid-19 positiv getesteten Person unter Quarantäne und dürfen vorerst gar nicht in die Firma kommen. Wir haben einige interessante Punkte zur Digitalisierung im Home-Office zusammengestellt, die Sie beachten sollten.

Zeiteinsparung und konzentriertes Arbeiten

Home-Office bietet hier einige Vorteile. Gerade in der IT besteht die Möglichkeit, dringende Probleme direkt von zu Hause aus zu lösen – ohne großen Zeitverlust durch eine lange Anfahrt.

Außerdem erhöht Home-Office die Zufriedenheit der eigenen Mitarbeiter. Auch die Suche nach neuen Mitarbeitern wird vereinfacht, wenn man als Firma mobiles Arbeiten anbieten kann. Die meist vermehrte Ruhe im eigenen Haus und die entfallende Zeit der Anfahrt zur Arbeit sorgen dafür, dass Home-Office beliebt ist. Die Mitarbeiter schätzen sich deutlich produktiver ein, weil sie in Ruhe an einer Sache arbeiten können – ohne dass ein Kollege in der Tür steht und sie in einer Konzentrationsphase stört.

Unser besonderer Vorteil war natürlich, dass wir schon seit Langem eine Lösung verwenden, mit der Mitarbeiter einfach und unkompliziert von daheim aus arbeiten können. Aber selbst wenn dem nicht so war und noch eine Lösung für Home-Office gefunden werden muss, sollte man dabei an den wichtigsten Punkt denken: Die Sicherheit!

Sicherheit bei der Datenübertragung

Jeder Mitarbeiter muss einen firmeneigenen Laptop erhalten. Die Festplatte wird dabei selbstverständlich vollverschlüsselt und das Anmelden sowohl am Laptop als auch am Firmen-VPN erfolgt mit Zwei-Faktor-Authentisierung. Alle Zertifikate, wie z.B. für das VPN oder sonstige Firmenserver, müssen gültig zertifiziert sein. Gerade im Home-Office ist ein „Man-in-the-Middle"-Angriff mit einem gefälschten Zertifikat schnell durchgeführt.

Womit wir zum nächsten Punkt kommen: Das verwendete Netzwerk muss bestmöglich abgesichert sein. Der heimische WLAN-Router muss mit einem starken Passwort versehen sein und auf offene WLAN-Netzwerke, z.B. im Café oder am Flughafen, verzichtet man besser. Notfalls erstellt man lieber selbst mit dem Handy einen WLAN-Hotspot und geht über die Handy Funkschnittstelle. LTE/4G gilt weiterhin als sicher!

Sperren Sie Ihren Computer

Genau wie in der Arbeit beachten Sie bitte ebenso zu Hause den Computer zu sperren, sobald Sie den Arbeitsplatz verlassen. Das betrifft auch ein kurzes Auffüllen der Kaffeetasse. Unbefugte dürfen zum Computer keinen Zugang haben. Auch wenn die eigenen Kinder es natürlich nicht böse meinen, wenn sie wichtige Daten löschen, aber so ein Vorkommnis kann große Probleme nach sich ziehen.

Backup wichtiger Daten

Das versehentliche Löschen von Daten betrifft gleich das nächste Thema: Backup!

Viele Firmen möchten auf den Rechnern der Mitarbeiter, sei es zu Hause oder in der Firma, möglichst keine Daten ablegen. Die Netzlaufwerke der Firma werden regelmäßig gesichert und gelten somit als sicher in puncto Datenverlust. Jetzt ist der richtige Zeitpunkt, die Sicherungen zu überprüfen – möglichst mit einem kompletten Rückspieltest!

VPN oder Fernwartungssoftware?

Was das Firmen-VPN betrifft, so sollten Sie vorab klären, wie es konfiguriert ist. Es kann den kompletten Netzwerkverkehr des Rechners über die Firma leiten oder nur den firmeninternen Netzwerkverkehr.

Sollten Sie also nebenbei ein wenig privat im Internet surfen, so ist es durchaus möglich, dass dies über die Netzwerkinfrastruktur der Firma läuft und die Firma davon nicht begeistert ist.

Zum Thema VPN sollte klar sein: Fernwartungs-Software spart das selbst konfigurierte VPN ein, hat aber auch Nachteile. Neben einem eventuell nicht ausreichend hohen Sicherheitsstandard kostet solche Software selbstverständlich Lizenzgebühren. Dies kann teuer werden, wenn viele Mitarbeiter gleichzeitig über die Software arbeiten.

Was ist eigentlich VPN?

Ein Virtual Private Network (VPN) ist im Prinzip nichts anderes als ein eigenes Netzwerk, welches innerhalb eines schon vorhandenen Netzwerkes erstellt wird. Virtuell ist es, weil hierzu keine neuen Leitungen gelegt werden müssen, sondern es über die vorhandenen Leitungen funktioniert.

Wenn wir heute von VPNs sprechen, dann meinen wir normalerweise nicht nur ein Netzwerk in einem Netzwerk, sondern auch ein entsprechend abgesichertes Netzwerk in einem unsicheren Netzwerk. Das unsichere Netzwerk ist hier zumeist das Internet, bei dem niemand sagen kann, ob irgendwo jemand sitzt, der unseren Datenverkehr abfangen, mithören oder verändern will.

Ein VPN hingegen baut über dieses unsichere Netzwerk eine sichere Verbindung auf. Dabei werden modernste Verschlüsselungstechniken genutzt, sodass sogar ein Geheimdienst, der den kompletten Verbindungsaufbau mithören könnte, trotzdem nur einen verschlüsselten Datenstrom sieht, mit dem er nichts anfangen kann.

Ein VPN sorgt hierbei nicht nur dafür, dass der Datenstrom verschlüsselt ist, sondern auch für eine Authentifizierung. Sie können sich also sicher sein, dass Sie sich tatsächlich mit Ihrer Firma verbinden und auch Ihre Firma weiß, dass Sie es sind.

Während die VPN-Verbindung besteht, ist es für alle angeschlossenen Computer und Systeme nicht ersichtlich, dass Sie sich nicht im gleichen Netzwerk der Firma befinden, sondern in Wirklichkeit vielleicht viele Kilometer entfernt. Einzig und allein die Verzögerung lässt ein VPN bemerken. So können Sie von zu Hause aus selbstverständlich den Firmendrucker verwenden, auf alle Server zugreifen oder Ihr VoIP-Telefon bedienen. Eingeschränkt wird das Ganze natürlich immer von verschiedensten komplexen Regelwerken, die auf Firmenseite exakt regeln, welcher Datenverkehr innerhalb der Firma bleibt und welcher ins VPN darf.

Hardware und Virenscanner

Was die Hardware betrifft, so ist ein von der Firma gestellter und entsprechend abgesicherter PC oder Laptop Pflicht. Der PC benötigt eine aktivierte Firewall, einen aktivierten Virenscanner und alle aktuellen Updates. Dies muss regelmäßig überprüft werden. Das Nutzen von Privat-PCs ist verlockend. Aus Sicherheitsaspekten sollte man aber davon absehen.

Sicheres Arbeiten

Cyberkriminelle nutzen die aktuelle Situation aus. Gleich zu Anfang der Corona-Krise haben wir ein deutlich erhöhtes Phishing- und Spamaufkommen bemerkt. Man sieht, dass hier auch versucht wird, aus dem Social Distancing der Mitarbeiter im Home-Office Profit zu machen. Die Mitarbeiter müssen ein Sicherheitsbewusstsein für dieses Thema besitzen. Ein schlecht abgesicherter Rechner im Home-Office stellt einen einfachen Eingangspunkt ins komplette Firmennetzwerk dar.

Und noch ein Tipp: Kommen Sie nicht auf die Idee, zu Hause Ihr privates Mailfach oder eine private Cloud-Lösung zu verwenden, um schnell Dateien auszutauschen. Firmendaten müssen unbedingt innerhalb der Kontrolle der Firma bleiben. Die DSGVO ist hier sehr strikt und sieht hohe Strafen vor. Sie sollten als Mitarbeiter keine Vorgaben unterwandern. Notfalls müssen Sie Ihren Vorgesetzten klar machen, was Ihnen fehlt, damit sie diesbezüglich Abhilfe schaffen können.

Der Autor

Foto: cimdata software GmbH

Thomas Christlieb, Softwareentwickler und IT-Experte bei cimdata software GmbH

Tools für Ihr Team

Als Firma sollte man selbstverständlich Tools zur Zusammenarbeit bereitstellen. Bekannt ist hierbei z.B. die freie Software „Nextcloud“ für Datei-, Kontakte-, und (Team-)Kalenderfunktionen. Während zum Beispiel „Rocket.Chat“ ein umfangreiches Chat-Tool bereitstellt, ermöglicht „Jitsi Meet“ Online Meetings mit oder ohne Webcam. Alle diese Lösungen sind Open Source und einfach auf einem eigenen Server zu hosten. Somit kommt man nicht in die Gefahr, gegen die DSGVO zu verstoßen. Auch hier setzt man auf offiziell signierte Zertifikate und ist damit rechtlich und sicherheitstechnisch auf der richtigen Seite.

Regelmäßiges Home-Office

Home-Office wird uns in der Arbeitswelt erhalten bleiben. Wenn man nicht komplett von zu Hause arbeitet, dann vielleicht ein paar Tage pro Woche, denn vielen Mitarbeitern fehlt im Home-Office der direkte Kontakt zu den Kollegen. Trotzdem bietet die Arbeit von zu Hause sowohl für Arbeitgeber und Arbeitnehmer Vorteile und wird weiterhin dazu gehören wie der Obstkorb und die Kaffeemaschine. Firmen, die ihren Mitarbeitern kein Home-Office anbieten, aber die technischen Möglichkeiten besitzen, werden auf dem Arbeitsmarkt das Nachsehen haben. *Christlieb/we*