Sicher arbeiten aus dem Home-Office

Und nun öfter im Home-Office... Wie funktioniert das am besten?

Viele Firmen stehen momentan vor dem gleichen Problem. Die Mitarbeiter, die es können, sollen von zu Hause aus arbeiten. Manche stehen vielleicht wegen Corona noch unter Quarantäne und dürfen nicht in die Firma kommen. Gut natürlich, wenn man schon seit Langem eine Lösung verwendet, mit der Mitarbeiter von daheim aus arbeiten können. Aber auch wenn man jetzt schnell eine eigene Lösung ausrollen muss, sollte man dabei gleich von vornherein an das Wichtigste denken: Die Sicherheit!

Sicherheit bei der Datenübertragung

Der Optimalfall ist natürlich, dass jeder Mitarbeiter einen firmeneigenen Laptop bekommt. Die Platte muss dabei (selbstverständlich!) vollverschlüsselt sein und das Anmelden sowohl am Laptop als auch am Firmen-VPN sollte mit Zwei-Faktor-Authentisierung funktionieren.

Alle Zertifikate (z.B. für das VPN oder sonstige Firmenserver) sollten 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 Netzwerk, welches man verwendet, sollte bestmöglich abgesichert sein. Der heimische WLAN-Router sollte mit einem starken Passwort versehen sein und auf offene WLAN-Netzwerke, z.B. im Café oder am Flughafen sollte man verzichten. Notfalls spannt man lieber selbst mit dem Handy einen WLAN-Hotspot auf und geht über die Handy Funkschnittstelle. LTE/4G gilt weiterhin als sicher!

Sperren Sie Ihren Computer

Genau wie in der Arbeit sollten Sie den Computer sperren, sobald Sie den Arbeitsplatz verlassen. Das betrifft auch kurzes Kaffeeholen. Unbefugte sollten zum Computer möglichst gar keinen Zugang haben. Auch wenn die eigenen Kinder es natürlich nicht böse meinen, wenn sie wichtige Daten löschen, aber das kann große Probleme nach sich ziehen.

Backup wichtiger Daten

Was gleich das nächste Thema betrifft: Backup!

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

Sicherlich spricht nichts dagegen, die Daten auch daheim auf Ihrer (vollverschlüsselten!) Festplatte zu speichern, wenn es denn keine aktuellere Version als in der Firma ist und wenn die Firma mit der Sicherung einverstanden ist.

VPN oder Fernwartungssoftware?

Was das Firmen-VPN betrifft, so sollten Sie 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 diese davon nicht begeistert ist.

Zum Thema VPN sollte klar sein: Fernwartungs-Software wie Teamviewer oder AnyDesk ist schön, hat aber auch Nachteile. Neben einem eventuell nicht ausreichend hohen Sicherheitsstandard kostet solche Software selbstverständlich Lizenzgebühren und wenn man viele Mitarbeiter gleichzeitig über die Software arbeiten lassen will, so kann das teuer werden. Teamviewer wird z. B. per gleichzeitige Sitzungen bezahlt. Außerdem braucht jeder Mitarbeiter einen Rechner in der Firma, auf den er sich einwählen kann. Dies kann natürlich ein Terminalserver sein, aber auch dann werden wieder Lizenzgebühren fällig.

Hardware und Virenscanner

Was die Hardware betrifft, so ist ein von der Firma gestellter und entsprechend abgesicherter PC wünschenswert. Der PC sollte eine aktivierte Firewall, einen aktivierten Virenscanner und alle aktuellen Updates besitzen. Dies sollte 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 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. 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 sollten 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.

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. Rocket.Chat stellt ein umfangreiches Chat-Tool bereit und Jitsi Meet ermöglicht 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.