

Sicherheitsempfehlungen für die Arbeit im Homeoffice

Mit der Arbeit im Homeoffice tun sich neue Sicherheitsrisiken auf, die es zu minimieren gilt. Viele dieser Risiken ergeben sich aus der Varianz der von den Mitarbeitern eingesetzten privaten IT-Geräten. Aber auch die Anfälligkeit gegenüber zielgerichteten Phishing-Attacken ist im Homeoffice deutlich erhöht. Die Arbeitsweise der im Homeoffice eingesetzten Mitarbeiter sollte daher nach Sicherheits Gesichtspunkten analysiert und reguliert werden.



Sichere Infrastruktur

Gewährleistung eines sicheren Arbeitsplatzes, der den Einblick Unbefugter (z. B.: Mitarbeiter, Familienmitglieder) in sensible Daten zuverlässig verhindert. Ein starkes Passwort kombiniert mit einer Zwei-Faktor-Authentifizierung (z. B. Duo Security) ist dringend empfehlenswert. Eine VPN-Anbindung des Heimarbeitsplatzes bietet zuverlässig abgesicherte Kommunikationskanäle.



Schutz vor Schadcode und Phishing

Eine maximale End-Point-Security (z.B. Kaspersky Endpoint Security for Business Advanced) und Malware-Protection (z.B. Malwarebytes) sind dringend erforderlich. Es ist in Zeiten der Corona-Pandemie vermehrt mit Phishing zu rechnen, wobei gefälschten Websites, Emails oder Kurznachrichten eingesetzt werden, um persönliche Daten einzusehen oder manipulieren zu können.



Zuverlässige Kommunikation

Die zulässigen Kommunikationswege müssen von allen Beteiligten eingehalten werden. Es muss die Möglichkeit geben, die Kommunikation z.B. über einen zweiten Kanal - wie Telefon oder Chat (z.B. mit der 3CX-TK-Anlage) – im Verdachtsfall zu verifizieren.



Klare Sicherheitsregelungen

Die Aufstellung unmissverständlicher und transparenter IT-Sicherheitsregeln durch die Geschäftsführung ist unabdingbar. Ein entsprechendes Dokument ist zu fertigen und an alle Beteiligten zu übermitteln.