

So geht sicheres Homeoffice

Achtung Hacker-Angriffe: Der Datenschutzexperte Mathias Past gibt Tipps für ein sicheres Homeoffice



Homeoffice ist auch eine massive Frage der Sicherheit. Darauf macht Ingeborg Dockner, die Obfrau der Sparte „Information & Consulting“ der WKNÖ, aufmerksam. „Unternehmen sind gut beraten, beim Homeoffice nicht nur auf Arbeitszeiten etc. zu achten, sondern gemeinsam mit ihren MitarbeiterInnen auch klare Sicherheitsstandards für ihre Daten zu fixieren.“ Denn, so Dockner: „Mit der weiteren Zunahme von Homeoffice werden mit Sicherheit auch die kriminellen Versuche von Hackern, über Sicherheitslücken beim Homeoffice an Daten, Firmengeheimnisse und Geld heranzukommen, steigen.“

Verschlüsselung der Festplatte - keine betriebsfremden USB-Sticks

Für Datenschutzexperten Mathias Past ist besonders wichtig, dass beim Homeoffice ausschließlich firmeneigene Geräte mit genehmigter Software zum Einsatz kommen. „Die Verschlüsselung der Festplatte sollte dabei jedenfalls Standard sein“, betont Past. Der Zugriff auf das firmeneigene Netzwerk vom Heimarbeitsplatz aus sollte immer über eine Virtual Private Network (VPN)- Lösung erfolgen, da nur so sichergestellt werden könne, dass vertrauliche Dokumente und Kommunikation nicht mitgelesen bzw. manipuliert werden können. Entsprechend ist auch die Verwendung von betriebsfremden Wechseldatenträgern wie USB-Sticks ein No-Go.

Nicht nur Hacker - Gefahrenherd offenes Fenster

Entscheidend für sicheres Homeoffice ist aber auch, dass die MitarbeiterInnen darauf achten, dass nur sie Zugang zum Computer haben. Auch bei nur kurzen Pausen, bei denen der Arbeitsplatz verlassen wird, muss der Computer folglich gesperrt werden. Allfällig offene Fenster sind zu schließen. Ausreichende Sicherungskopien, am besten über die zentralen Systeme des Unternehmens, sind ein Muss. Es müsse, etwa über regelmäßige Schulungen, im Unternehmen ein Sicherheitsbewusstsein geschaffen werden. Das sei der Schlüssel zum Erfolg.

Besuchen Sie uns auf: fleischundco.at