



Geschäftsführerin Petra Michalczak-Hülsmann | T 02521 85050 | www.gfw-waf.de

Presseinformation

Wie man Cyberattacken abwehrt

gfw-Lunchtalk zum Schutz vor den Gefahren wachsender Digitalisierung

Mit zunehmender Digitalisierung in Unternehmen steigt die Gefahr, Opfer einer gezielten oder ungezielten Cyberattacke zu werden. „Die Auswirkungen können verheerend sein bis hin zu einem kompletten Betriebsstillstand“, sagte Petra Michalczak-Hülsmann am Dienstag (22. November) beim mittäglichen Online-Format „Lunchtalk“ der Gesellschaft für Wirtschaftsförderung im Kreis Warendorf. Die gfw-Geschäftsführerin hatte kleinere und mittlere Unternehmen eingeladen, um deren Widerstandsfähigkeit gegenüber Cyber-Attacken zu erhöhen.

Die Gefahrenereinschätzung bestätigte Referent Arbnor Memeti, IT-Sicherheitsexperte und Berater für digitale Sicherheit bei Digital.Sicher.NRW, das vom nordrhein-westfälischen Wirtschaftsministerium beauftragte Zentrum für digitale Sicherheit in Unternehmen, vor den knapp 20 Teilnehmern. Neun von zehn Unternehmen seien in den vergangenen Jahren von Cyberattacken betroffen gewesen. Jedes zehnte Unternehmen sehe sich in einem solchen Fall existentiell gefährdet. Digital.Sicher.NRW berät Unternehmen auch individuell, kostenfrei und produktneutral, wie Memeti sagte.

Es war eine Fülle an Gefahren, über die der IT-Sicherheitsexperte aus der Praxis berichtete. Mobiles Arbeiten („Laptops lassen sich leicht aus Entfernung einsehen“) gehört ebenso dazu wie die Vorspiegelung falscher Identitäten, um Geldüberweisungen zu manipulieren. Zur regelrechten Seuche entwickeln sich Lösegelderpressungen. „Wer Daten hat, der muss mit Angriffen rechnen.“ Vor zwei Jahre besaßen 37 Prozent der Unternehmen angreifbare Daten, im vergangenen Jahr waren es schon 75 Prozent. Im Fall von Lösegeldzahlungen in durchschnittlicher Höhe von 255.000 Euro bekamen nur 64 Prozent der Betroffenen ihre Daten zurück. Trotz Zahlung betrug der durchschnittliche Gesamtschaden 1,64 Mio. Euro.

Zur Abwehr empfahl Memeti Antivirenprogramme und Spamfilter, sichere Identitäten mit sich nicht wiederholenden Passwörtern („Mindestens zwölf Zeichen“), Mitarbeiterschulung, Software-Updates auf neustem Stand, regelmäßige Backups und Datensicherungen.

22. November 2022