Für mehr IT-Sicherheit im Homeoffice: WFG lädt Unternehmen zu Onlineveranstaltung mit Experten ein

Markus Gringel

Durch die Corona-Pandemie sind mobiles Arbeiten und Homeoffice für viele Beschäftigte im Kreis Unna von der Ausnahme zur Regel geworden. Damit die Arbeit von zu Hause nicht zur Datenfalle wird, befasst sich die Onlineveranstaltung „IT-Sicherheit im Homeoffice“, zu der die Wirtschaftsförderung Kreis Unna (WFG) für Dienstag, 11. Mai 2021 von 9.30 bis 11.00 Uhr einlädt, mit dem Schutz vor Cyberkriminalität am heimischen Schreibtisch.

Wie sicher sind sensible Unternehmensdaten, wenn die Kolleginnen und Kollegen von zu Hause aus arbeiten? Welche Sicherheitslücken gibt es und wie lässt sich eigentlich eine geschützte IT-Struktur implementieren? Diesen und vielen weiteren Fragen gehen die drei Referenten in ihrem Kurzvortrag nach. So thematisiert Prof. Dr.-Ing. Jan Pelzl (Hochschule Hamm Lippstadt – Lehrgebiet „Computer Security“) wie die Mitarbeiter*innen im Unternehmen beim Thema ITSicherheit mitgenommen werden können. Markus Gringel (SECUDOS GmbH,

Kamen)
zeigt aus der Praxis, wie eine praktische und technische Umsetzung von ITSicherheit im Homeoffice aussehen kann. Sollte der Worst-Case dann doch eintreten, helfen die Tipps von Thomas Müller (Sparkasse Hamm) weiter, der finanzielle Absicherungsmöglichkeiten von IT-Sicherheitsrisiken aufzeigt.

Anmeldungen sind per E-Mail an veranstaltung@wfg-kreis-unna.de möglich. Die Veranstaltung findet im Rahmen des Projekts „Wissen schafft Erfolg" in Kooperation mit der Wirtschaftsförderung Hamm und der Sparkasse Hamm statt. Das Projekt wird gefördert durch Mittel der Europäischen Union und des Landes NRW.

Kurzinterview mit Markus Gringel, IT-Experte und Referent bei der Veranstaltung

Was ist das größte Sicherheitsrisiko beim mobilen Arbeiten bzw. im Homeoffice?

Markus Gringel: „Die Mitarbeiter*innen und deren Bequemlichkeit sind das größte Risiko. Viele Beschäftigte haben beispielsweise keine
Lust, ein zehnstelliges Passwort mit Sonderzeichen und Zahlen zu verwenden und dieses dann auch noch regelmäßig zu wechseln. Zudem
benutzen viele Mitarbeiterinnen und Mitarbeiter*innen zum Datenaustausch oftmals Cloud-Dienste, die nicht mit der Datenschutzgrundverordnung (DSGVO) konform sind. Das hat der Arbeitgeber gar nicht unter Kontrolle. Hinzu kommt die oftmals fehlende
Sicherheitsumgebung am heimischen Schreibtisch: Viele Beschäftigte nutzen im mobilen Arbeiten den Firmen-Laptop und das private
W-Lan. Dann haben die Nutzer aber keine Firewall und der VPNZugang ist das Einfallstor für Hacker in das Firmennetzwerk. Man
muss immer beide Themenbereiche berücksichtigen: Sicherheit

und Schutz!“

Wie lässt sich das Arbeiten von zu Hause mit einfachen Mitteln sicherer machen?

Markus Gringel: „Ein ausreichend starkes Passwort des Benutzeraccounts auf dem Endgerät des Mitarbeiters/der Mitarbeiterin kann schon sehr viel bewirken. Auch das Sperren des Computers beim Verlassen des Arbeitsplatzes ist schnell gemacht und hilft. Wenn das Unternehmen sich dann noch dazu entscheidet, eingebettete ITLösungen zu nutzen, die auf dem eigenen Server liegen und die es selbst unter Kontrolle hat, anstatt auf Cloud-Lösungen zurückzugreifen, ist im Bereich Sicherheit viel gewonnen.“

Was raten Sie Unternehmen bezüglich der IT-Sicherheit?

Markus Gringel: „Ich rate vor allem dazu, die Beschäftigten mitzunehmen und sie für das Thema zu sensibilisieren, ihnen beispielsweise begreiflich zu machen, warum ein starkes Passwort zwar nervig, aber für die Sicherheit des Betriebs unausweichlich ist. Wichtig ist es, die Prozessabläufe der Beschäftigten zu verstehen und sie sicher und gleichzeitig leicht handhabbar zu machen. Darüber hinaus rate ich dazu, Sicherheitsmaßnahmen zu ergreifen, sodass das Unternehmen die Daten selbst unter Kontrolle hat und Herr über die Daten ist und bleibt.“