„Wir haben unsere Bankverbindung geändert.“ – Neue Betrugsmasche bei Rechnungsstellung per E-Mail

In Deutschland breitet sich gerade eine neue Betrugsmasche aus, von der bereits viele Unternehmer betroffen sind: Eine harmlose Mail, in der ein Geschäftspartner mitteilt, er habe angeblich seine Bankverbindung geändert. Überweist man dann offene Rechnungsbeträge auf dieses neue Konto, haben die Betrüger gewonnen. Wichtige Tipps vom LKA Baden-Württemberg.

Das Landeskriminalamt von Baden-Württemberg hat folgende Warnung für Unternehmer herausgegeben:

„Wir haben unsere Bankverbindung geändert.“ – Neue Betrugsmasche bei Rechnungsstellung per E-Mail

Eine Betrugsmasche, die im asiatischen Raum schon seit einiger Zeit bekannt ist, verbreitet sich nun auch zunehmend in Deutschland: Betrug bei Rechnungsstellung per E-Mail. In Zeiten des elektronischen Zahlungsverkehrs werden Rechnungen in vielen Geschäftsbereichen nur noch elektronisch versandt. Diesen Umstand machen sich nun auch Kriminelle zu nutzen, indem sie böswillig auf den Nachrichtenaustausch zwischen Verkäufer/Dienstleister und Kunde einwirken.

Die Täter nutzen hierzu verschiedene Methoden, um sich in die Kommunikation einzuschalten. Eines haben alle Vorgehensweisen jedoch gemeinsam: Die Mitteilung an den Kunden, dass sich die Bankverbindung des Rechnungsstellers angeblich geändert habe. Ist dieses Täuschungsmanöver beim Kunden erfolgreich, überweist dieser den tatsächlich offenen Rechnungsbetrag auf das Konto der Betrüger.

Woher wissen die Täter, dass eine offene Forderung besteht, und wie schalten sie sich in die Kommunikation ein?

Die Kriminellen „hacken“ sich auf einen der beteiligten E-Mail-Server ein, fangen die relevanten E-Mails ab und verändern die Inhalte ganz oder teilweise. So gaukeln sie den Kunden eine E-Mail vom Rechnungssteller vor, aus der hervorgeht, dass sich dessen Bankverbindung geändert habe.

Auf diese Weise manipulieren die Täter auch bei andauerndem E-Mail-Verkehr die Kommunikation so, dass bei Rückfragen per E-Mail der Betrug zunächst unentdeckt bleibt. Der Polizei sind außerdem Fälle bekannt, in denen die Betrüger zusätzlich gefälschte Dokumente per Briefpost verschickten, um die Glaubwürdigkeit des manipulierten E-Mail Verkehrs zu untermauern.

Um einem solchen Betrug vorzubeugen, rät das LKA Baden-Württemberg daher zu folgenden Maßnahmen:
Sensibilisieren Sie Ihre Mitarbeiter gegenüber dieser Betrugsmasche.

Überprüfen Sie E-Mails mit Rechnungen sorgfältig auf den richtigen Absender und die korrekte Schreibweise der E-Mail Domain.
Prüfen Sie bei verdächtigen E-Mails die vorliegenden Informationen über einen zweiten

Kommunikationskanal. Nutzen Sie statt E-Mail hierzu z.B. das Telefon.
Halten Sie Ihre Software stets auf dem neuesten Stand (beispielsweise durch ein Patchmanagementsystem).
Weisen sie prophylaktisch in Ihrer geschäftlichen E-Mail Signatur darauf hin, dass Sie Ihren Kunden eine Änderung der Bankverbindung niemals via E-Mail mitteilen werden.
Wenn möglich, nutzen Sie digitale Signaturen.
Bereiten Sie sich trotz Ihrer Sicherheitsmaßnahmen auf den Schadensfall vor. Teil Ihres Notfallplanes sollte die sofortige Einbeziehung Ihrer Hausbank und der Zentralen Ansprechstelle Cybercrime (ZAC) sein.

Zentrale Ansprechstelle Cybercrime
beim Landeskriminalamt Baden-Württemberg.

Die ZAC dient als zentraler Ansprechpartner für die Wirtschaft und Behörden in allen Belangen des Themenfeldes Cybercrime.
E-Mail: cybercrime@polizei.bwl.de