Das Bundeskriminalamt warnt vor einer neuen Welle von Betrugshandlungen gegen österreichische Unternehmen.

Das Bundeskriminalamt warnt aus aktuellem Anlass im Rahmen von „**GEMEINSAM.SICHER in Österreich**“ vor einlangenden Geschäfts E-Mails, die eine Änderung der Zahlungsverbindung, kurz der Kontonummer zum Inhalt haben.

Gerade in Zeiten in denen das Homeoffice vermehrt genutzt wird, zielen die Täter darauf ab, mit E-Mails Mitarbeiterinnen und Mitarbeiter von Unternehmen zu täuschen und ihre Opfer zu Zahlungen auf falsche Konten zu verleiten.

Bei diesem Phänomen, das international als BEC (Business E-Mail Compromise) bezeichnet wird, sind zumeist Unternehmen, die internationale Geschäftsbeziehungen pflegen, das Ziel dieser Angriffe.

Dabei übernehmen die Täter entweder das E-Mail-Konto einer Partnerfirma oder er erstellen ein eigenes E-Mail-Konto, das der echten E-Mailadresse nahezu gleicht. Die Täter agieren damit vermeintlich im Namen des eigentlichen Geschäftspartners und ersuchen ihre Opfer zukünftige oder ausstehende Zahlungen auf ein anderes Bankkonto als üblich zu überweisen. So werden die Zahlungen auf ein Konto der Täter umgeleitet und schnellstmöglich weitertransferiert oder behoben.

Glück im Unglück hatte ein renommiertes österreichisches Unternehmen im April und Mai dieses Jahres: Dieses Unternehmen erhielt von einem angeblichen Partnerunternehmen die Mitteilung, dass das Verrechnungskonto für Zahlungen geändert wurde. Die verwendete E-Mail-Adresse wurde jedoch von den Tätern eigens angelegt und unterschied sich lediglich in einem einzelnen Buchstaben von der tatsächlichen E-Mailadresse des Geschäftspartners. Trotz Einhaltung interner Sicherheitsmechanismen gelang es den Tätern, das Unternehmen zu Zahlungen von insgesamt EURO 600.000 zu bewegen. Da jedoch die Zahlungsdetails der Täter unrichtig waren, wurde der Betrug in letzter Minute noch bemerkt und die Zahlungen retourniert.

Aufgrund der jetzt wieder verstärkt auftretenden Betrugshandlungen nach diesem Muster werden folgende Tipps gegeben:

- Achten Sie auf einlangende Ersuchen, die die Änderung der Zahlungsverbindungen bekannt geben und verifizieren Sie diese jedenfalls, bevor Sie die nächste Zahlung leisten.
- Verwenden Sie für die Verifizierung unbedingt einen anderen Kommunikationskanal, als den, über den der Änderungswunsch eingelangt ist.
- Versuchen Sie, Ihnen persönlich bekannte Personen aus Partnerunternehmen, über die Ihnen bereits bekannten und bereits genutzten Kontaktdaten zu erreichen.
- Überprüfen Sie kritisch die Schreibweise von E-Mailadressen von Absendern.
- Sind Sie sich bewusst, dass E-Mailadressen leicht gefälscht werden können. Diese Vorgehensweise nennt man „Spoofing“. Auch wenn die Schreibweise exakt jene ist, die Sie von Ihrem Partner kennen, muss es sich nicht zwingend um jene von Ihrem Geschäftspartner handeln.
- Achten Sie auf die Änderungen in der Kommunikation. Rechtschreibfehler, unübliche Formulierungen oder ein ungewöhnlicher Wechsel zwischen „Sie“ und „Du“ könnten ein Anzeichen für einen Täuschungsversuch sein.
- Wenn Sie bereits Opfer eines derartigen Betruges wurden, kontaktieren Sie schnellstmöglich Ihre überweisende Bank, um das Geld zurück zu fordern und erstatten Sie Anzeige auf der nächstgelegenen Polizeiinspektion.

Bundesministerium Inneres

POLIZEI
KRIMINALPRÄVENTION

GEMEINSAM.SICHER
in Österreich