



Warnung vor gefälschten E-Mails

Sehr geehrte Damen und Herren,
aus aktuellem Anlass, bei dem versucht wurde, Gelder durch einen Schatzmeister einer Jägerschaft auf ein unberechtigtes, fremdes Konto transferieren zu lassen, möchten wir Sie präventiv auf die so genannte "CEO-Fraud" Masche (Chef-Betrug) aufmerksam machen. Diese Betrugsmasche ist nicht neu, scheint aber derzeit „wiederaufzuflackern“. In dem aktuellen Fall wurde dabei der Eindruck erweckt, der Absender der Betrugs-E-Mail sei die, von der LJN den Jägerschaften zur Verfügung gestellte Weiterleitungsadresse, „*jägerschaft*“@ljn.de.

Ursprüngliches Ziel der Betrugsversuche sind Firmen, in denen dem Finanzverantwortlichen eine angebliche Mail eines Weisungsbefugten/Chefs zugeht. Die Absenderadresse und die Ansprache stimmen oft sehr genau mit den internen bekannten Gepflogenheiten überein. In der Mail wird eine Überweisung für einen angeblich wichtigen Vorgang zuerst angefragt und bei erfolgter Antwort dann mit ausländischen Kontodaten auch eingefordert. In besonders dreisten Fällen wird temporäre Abwesenheit vorgeschoben (Meeting, Urlaub, Verlust von Handy), um anschließend den Kontakt über eine angeblich autorisierte dritte Person, z.B. Anwaltskanzlei, fortzuführen.

Weder die Mail noch der vermeintlich echte Absender noch der Anwalt sind echt! Wird das Geld tatsächlich auf das angegebene Konto überwiesen, ist das Geld in den allermeisten Fällen verloren.

An die notwendigen Informationen über Empfänger und Absender, dessen Identität gefälscht wird, gelangen die Betrüger über "Social Engineering", also z.T. akribische Vorabrecherchen in sozialen Medien, auf der Homepage des Unternehmens oder über Berichte in Printmedien. Kombiniert ergeben diese Informationen oft umfangreiche und für die Betrüger wertvolle Hinweise, welche Personen für Finanzen verantwortlich sind, wie sie erreichbar sind und wer ihnen gegenüber weisungsbefugt ist.

Schützen Sie sich vor dieser Betrugsmasche, indem Sie bei ungewöhnlichen Zahlungsanfragen skeptisch sind und über einen zweiten Kanal, z.B. per Anruf unter einer Ihnen bekannten und dem Absender zugehörigen Telefonnummer, zu dem Vorgang Rückfrage halten. Lassen Sie sich auf keinen Fall unter Zeitdruck setzen und verwenden Sie zur Kommunikation niemals in der E-Mail angegebene unbekannte Mailadressen oder Telefonnummern.

Weiterführende Informationen:

Warnung des BSI (Bundesministeriums für Sicherheit in der Informationstechnik):

https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/CEO_Fraud_10072017.html

Flyer (PDF) des BKA (Bundeskriminalamt) zur Prävention:

<https://www.bka.de/SharedDocs/Downloads/DE/IhreSicherheit/CEOFraud.pdf>