TLP:Clear

Warnung vor Betrugs-E-Mails zur Änderung von Kontodaten

Die Warnung wurde uns durch das LSI Bayern zur Verfügung gestellt
(LSI = Landesamt für Sicherheit in der Informationstechnik)

Zusammenfassung
Dem LSI sind aktuell vermehrt betrügerische E-Mails bekannt, die mit gefälschtem Absender zielgerichtet zu einer Änderung von Bankdaten und anschließend einer gefälschten Überweisung an diese neuen Bankdaten verleiten wollen.

Sachverhalt
Es liegen aufgrund mehrerer Meldungen Kenntnisse über betrügerische E-Mails vor.
Es wird vermeintlich im Namen eines bekannten Geschäftspartners gezielt eine E-Mail an den zuständigen Ansprechpartner in Vergabestellen und Verwaltungen verschickt. In diesen E-Mails wird mit Nachdruck aufgefordert, die Bankdaten für zukünftige Überweisungen zu ändern.
Wenn es sich um Rechnungsinformationen handelt, erbeuten die Kriminellen diese oft durch einen gezielt vorgeschalteten Social Engineering Angriff beim Lieferanten oder Dienstleister der eigentlichen Zielorganisation. Dabei geben sich die Angreifer als Mitarbeiter der Zielorganisation aus und fragen noch offene Rechnungen an. Über diesen Weg erbeutete Rechnungsinformationen werden dann manipuliert und mit geänderten Kontodaten an die Zielorganisation gesendet.

Angreifer missbrauchen neben dem erwähnten Vorgehen aktuell auch Drittplattformen für legitim wirkende E-Mails. Dafür können zum Beispiel eingebettete Kontaktformulare dienen. Konkret wurde hierfür kürzlich die europäische Ausschreibungsplattform TED genutzt. In den bekannten Fällen nutzten Angreifende speziell hierfür registrierte Mailadressen zur Anmeldung auf einer Drittplattform. Die Ausschreibenden erhalten bei Kontaktaufnahme über diese Plattformen eine E-Mail von einer Mailadresse des Plattform-Betreibers, allerdings mit dem Inhalt des Angreifers. Dabei wird im "Reply-To:"-Feld die Mailadresse des Angreifers gesetzt. Hierbei soll der Angriff initial eingeleitet werden. Also die erste Kontaktaufnahme mit dem Dienstleister, der an der Ausschreibung teilgenommen hat, um so die nächsten Schritte wie Kontodaten und Betragsänderungen einzuleiten.

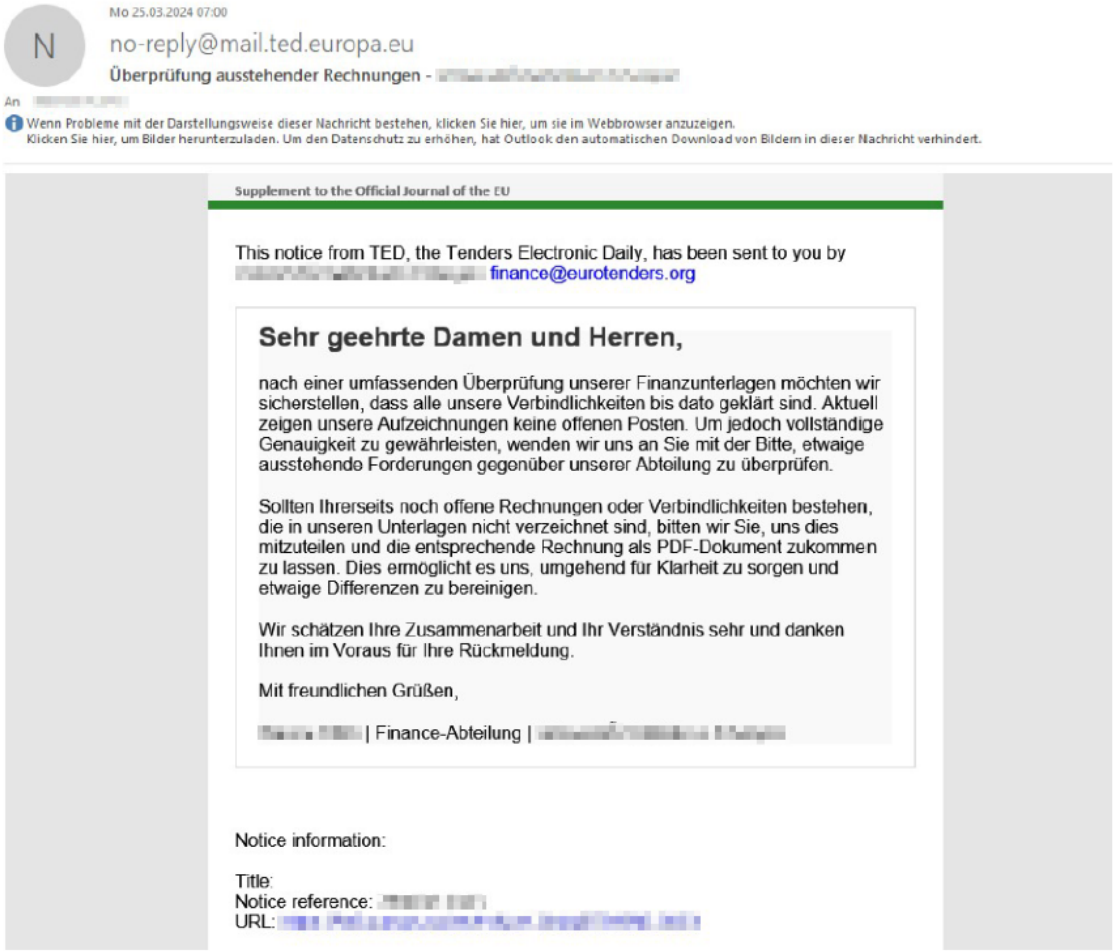
Die bisher bekannten Absender der E-Mail waren:
- @kreditorenbuchhaltung.net
- @kreditoren-buchhaltung.com
- @finanzbuchaltung-fibu.de
- @kpmgfinancecontrol.com
- @finance-asp1.com

Es sind aber auch beliebige andere Absenderadressen denkbar.
Im Betreff waren die folgenden Schlagwörter enthalten:
- Bankverbindung
- Änderung + Zahlung
- Anpassung + Zahlung

Auch hier sind alternative Formulierungen möglich.

Diese Betrugsmasche ist nicht neu und wird von Cyberkriminellen immer wieder verwendet. Auch in dieser Kampagne schreiben die Kriminellen ihre Opfer mit Nachdruck und gezielt an. Letzteres deutet auf abgeflossenen Mailverkehr oder das Abgreifen der benötigten Informationen von der Webseite des Opfers bzw. von öffentlich einsehbaren Informationen auf den Ausschreibungsplattformen hin.

Empfehlung
Wir empfehlen, alle Mitarbeiter – speziell jene im Vergabe- und Finanzbereich – entsprechend zu sensibilisieren.
Weisen Sie auch Ihre Lieferanten und Dienstleister auf diese Methode der Informationsgewinnung mittels Social Engineering hin.
Kontoänderungen sollten grundsätzlich gegengeprüft werden, beispielsweise durch tel. Rückruf beim etablierten Ansprechpartner oder einer Bestätigung von offizieller Stelle.



Mo 25.03.2024 07:00

N

no-reply@mail.ted.europa.eu

Überprüfung ausstehender Rechnungen -

An

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.
Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

Supplement to the Official Journal of the EU

This notice from TED, the Tenders Electronic Daily, has been sent to you by finance@eurotenders.org

Sehr geehrte Damen und Herren,

nach einer umfassenden Überprüfung unserer Finanzunterlagen möchten wir sicherstellen, dass alle unsere Verbindlichkeiten bis dato geklärt sind. Aktuell zeigen unsere Aufzeichnungen keine offenen Posten. Um jedoch vollständige Genauigkeit zu gewährleisten, wenden wir uns an Sie mit der Bitte, etwaige ausstehende Forderungen gegenüber unserer Abteilung zu überprüfen.

Sollten Ihrerseits noch offene Rechnungen oder Verbindlichkeiten bestehen, die in unseren Unterlagen nicht verzeichnet sind, bitten wir Sie, uns dies mitzuteilen und die entsprechende Rechnung als PDF-Dokument zukommen zu lassen. Dies ermöglicht es uns, umgehend für Klarheit zu sorgen und etwaige Differenzen zu bereinigen.

Wir schätzen Ihre Zusammenarbeit und Ihr Verständnis sehr und danken Ihnen im Voraus für Ihre Rückmeldung.

Mit freundlichen Grüßen,

| Finance-Abteilung |

Notice information:

Title:
Notice reference:
URL: