Aktueller Hinweis der Zentralen Ansprechstelle Cybercrime für die nds. Wirtschaft (ZAC)

Warnung vor betrügerischen E-Mails im Zusammenhang mit Ausschreibungen

09.07.2025

Beschreibung der Betrugsmasche
Derzeit nutzen Cyberkriminelle ausgelesene Daten von Vertragspartnern, um ausschreibende Unternehmen - mittels manipulierter Rechnungen - um ihr Geld zu betrügen. Hierfür nutzen die Täter Daten der Online-Plattform: **TED**. Diese Webseite ist eine zentrale Plattform für die Veröffentlichung öffentlicher Aufträge auf EU-Ebene. Sie bietet u. a. Zugang zu Informationen bzw. Bekanntmachungen über Ausschreibungen, die von EU-Institutionen und anderen öffentlichen Auftraggebern veröffentlicht werden.

Das Vorgehen der Täter
Im ersten Schritt werden die Gewinner von Ausschreibungen per E-Mail kontaktiert. Diese E-Mails sind kurz und knapp formuliert und enthalten die Aufforderung, offene Rechnungen zu übersenden. Die auf diesem Weg erlangten - legitimen - Rechnungen werden daraufhin von den Betrügern manipuliert, indem die Bankverbindung ausgetauscht wird.

Anschließend werden die veränderten bzw. manipulierten Rechnungen per E-Mail an die ausschreibenden Unternehmen, d. h. an die tatsächlichen Schuldner versandt. Im Falle einer Überweisung auf die geänderte Bankverbindung landet somit die Zahlung auf dem Bankkonto der Betrüger bzw. eines von den Betrügern eingesetzten Finanzagenten.

Die hier benannte Betrugsmasche lässt sich unter dem Phänomen Rechnungsmanipulation bzw. „Business-E-Mail Compromise“ subsumieren. Der ZAC sind aktuelle Fälle bekannt bei denen sehr hohe Summen tatsächlich erfolgreich auf betrügerische Bankkonten überwiesen wurden – oftmals handelt es sich um Beträge im 6-stelligen Bereich.

Allgemeine Informationen
Business-E-Mail Compromise (BEC) ist eine Form des E-Mail-Betrugs. Dabei nehmen Angreifer gezielt Unternehmen ins Visier, um Geld oder sensible Daten zu stehlen. Diese Betrugsmasche, auch Spear-Phishing genannt, täuscht oft die Identität eines Mitarbeiters oder Geschäftspartners vor, um den Empfänger zu bestimmten Handlungen zu bewegen. BEC ist ein ernsthaftes und wachsendes Problem, das Organisationen aller Größen und Branchen weltweit betrifft.

Es wird häufig verwendet, um finanzielle Transaktionen auszulösen oder an vertrauliche Informationen zu gelangen.
Rechnungsmanipulation bezeichnet eine betrügerische Veränderung oder Fälschung von Rechnungen, um sich oder anderen einen finanziellen Vorteil zu verschaffen oder das Unternehmen zu schädigen.

Empfehlungen zum Schutz

- **Prüfen Sie Absender-E-Mails sorgfältig:** Achten Sie auf Unstimmigkeiten wie unbekannte

Domains, Rechtschreibfehler oder abweichende E-Mail-Adressen. Kontaktieren Sie den Absender bei Zweifel direkt über bekannte, offizielle Kommunikationswege.

- **Verifizieren Sie Zahlungsaufforderungen:** Überprüfen Sie Rechnungen und Bankverbindungen vor jeder Zahlung. Kontaktieren Sie den Gläubiger telefonisch oder über verifizierte Kanäle, um die Echtheit der Forderung und der (geänderten) Bankdaten zu bestätigen.
- **Melden Sie verdächtige Aktivitäten:** Informieren Sie bei verdächtigen E-Mails oder Rechnungen umgehend Ihre IT-Abteilung, Ihre Bank sowie die zuständigen Behörden.
- **Schulen Sie Ihre Mitarbeitenden:** Sensibilisieren Sie Ihr Team für derartige Betrugsversuche und etablieren Sie klare Prozesse für die Prüfung von Rechnungen und Zahlungsanweisungen.

Handlungsempfehlungen

Sollten Sie bereits Opfer eines solchen Betrugs geworden sein, setzen Sie sich unverzüglich mit Ihrer Bank in Verbindung, um Zahlungen zu stoppen oder zurückzubuchen. Außerdem sollten Sie bei der Polizei eine Anzeige erstatten.

Die Strafanzeige können Sie über Ihre für Ihr Bundesland zuständige ZAC-Dienststelle, bei Ihrer Polizeidienststelle vor Ort oder z. B. über die Onlinewache der Polizei unter **Onlinewache** erstatten. Grundsätzlich empfehlen wir Ihnen wachsam zu bleiben und Ihre Geschäftsprozesse regelmäßig auf Sicherheitslücken zu überprüfen.

Permanenter Link zu diesem Artikel auf zac-niedersachsen.de:
https://zac-niedersachsen.de/artikel/83

Klicken Sie hier und abonnieren Sie unseren Newsletter.