Baden-Württemberg

LANDESKRIMINALAMT

**ZENTRALE ANSPRECHSTELLE CYBERCRIME**
**TELEFON 0711 5401-2444, FAX 0711 5401-2505**
**E-MAIL CYBERCRIME@POLIZEI.BWL.DE, INTERNET WWW.LKA-BW.DE/ZAC**

# Handlungsempfehlungen gegen E-Mail-Betrug

**20. September 2021**

Nahezu alle Unternehmen sind von Betrugsversuchen betroffen. Die Betrüger nutzen vielfältige Methoden, um die Betroffenen zur Überweisung von Geldern zu verleiten. Wie gehen die Betrüger vor? Sie spähen sensible Rechnungsdaten aus den E-Mail-Postfächern der betroffenen Unternehmen oder der Geschäftspartner aus und manipulieren vorgefundene Rechnungsentwürfe. Die in der Rechnung angegebene **Bankverbindung wird verfälscht** und die manipulierte Rechnung an den Rechnungsempfänger weitergeleitet. Hierfür verwenden die Täter zumeist leicht veränderte E-Mail-Adressen, die den E-Mail-Adressen der Geschäftspartner zum Verwechseln ähnlich sehen. Wird die Manipulation nicht erkannt, überweisen die Rechnungsempfänger die Summe auf das von den Betrugstätern angegebene Konto.

Andere Betrugstäter täuschen die Identität von Geschäftspartnern vor und versenden E-Mails an Unternehmen mit der Mitteilung, für ausstehende Rechnungszahlungen habe sich die **Bankverbindung geändert** und teilen angeblich neue Bankdaten mit.

Ähnlich gehen Betrugstäter vor, die den Namen eines Mitarbeiters im Unternehmen vortäuschen und der Personalstelle eine angeblich **geänderte Bankverbindung für die Gehaltszahlung** mitteilen.

Auch der „**falsche Geschäftsführer**“,[1] der die Identität von Vorgesetzten vortäuscht und versucht, die Mitarbeiter der Zahlungsstelle zu einer angeblich dringenden Überweisung zu verleitet, tritt nach wie vor in Erscheinung.

**Betrugsschaden im E-Mail-Rechnungsverkehr ist vermeidbar**. Die folgenden Empfehlungen tragen zur Abwehr von Betrugsversuchen bei und informieren über empfehlenswerte Sofortmaßnahmen beim Bekanntwerden eines E-Mail-Betrugs.

[1] https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/ceo-fraud

**Organisatorische Prävention**

- Bereiten Sie eine **Checkliste** mit allen notwendigen Arbeitsschritten nach der Feststellung eines Betrugsfalles vor. Stellen Sie die Liste allen zuständigen Mitarbeitern auch in ausgedruckter Form zur Verfügung.
- Die Checkliste sollte
  - interne Zuständigkeiten (z.B. Geschäftsführung, Vorgesetzte, Rechnungsstelle, IT-Abteilung, Rechtsvertreter) und
  - externe Zuständigkeiten (z.B. Hausbank, Polizei, IT-Dienstleister)

  beinhalten sowie deren jeweilige **Erreichbarkeit**.
- Betrügerische E-Mails werden zum Teil auch über die authentischen E-Mail-Adressen der Vorgesetzten oder Geschäftspartner versandt. Verlassen Sie sich niemals auf die Absender-E-Mail-Adresse, sondern gehen Sie kritisch mit jeder Rechnung mit hoher Forderung um.
- Definieren Sie betriebsintern eine kritische Summe für Rechnungsüberweisungen. Übersteigt eine eingehende Rechnung diese Summe, sollte das angegebene Zielkonto beim Rechnungssteller **telefonisch verifiziert** werden. Gleichen Sie gemeinsam mit Ihrem Geschäftspartner den Rechnungsvorgang und insbesondere das angegebene Zielkonto ab.
- Geht eine Nachricht mit der Mitteilung der angeblich **geänderten Bankverbindung** ein, sollte die angegebene Bankverbindung **in jedem Fall** telefonisch verifiziert werden.
- Kontaktieren Sie für die telefonische Verifizierung keinesfalls die in den Rechnungsdokumenten oder in E-Mails ersichtlichen Telefonnummern. In den E-Mails oder Rechnungen angegebene Telefonnummern können ebenfalls gefälscht sein und die entsprechenden Telefonanschlüsse von den Betrugstätern kontrolliert werden. Greifen Sie für die Telefonanrufe bei Ihren Geschäftspartnern auf das **eigene Adressverzeichnis** zurück.
- Die dringende Notwendigkeit der Verifizierung sollte allen Mitarbeiterinnen und Mitarbeitern, die berechtigt sind für
  - Zahlungen
  - zur Änderung von Stammdaten (Bankverbindung),

  als **verbindlicher Geschäftsprozess** vorgegeben werden.
- Auch wird die Dokumentation entsprechender Änderungsvornahmen der hinterlegten Stammdaten empfohlen (bspw. Zeitpunkt, Veranlasser, verifiziert

ja/nein, Name und Erreichbarkeit der bestätigenden Gegenseite, Angabe Verifizierungskanal, Ablage der eingegangenen Änderungsmitteilung).

**Verhaltensprävention für Mitarbeiterinnen und Mitarbeiter**

- Die Polizei empfiehlt die **Schulung der zahlungsberechtigten Mitarbeiter**. Empfehlenswerte Schulungsinhalte sind neben den bereits erwähnten Prozessvorgaben insbesondere die betriebsinternen Meldewege zur Kontaktierung Vorgesetzter oder der IT-Fachebene für die Mitteilung betrugsverdächtiger Vorkommnisse.
- Zur Vorbereitung des Betruges werden oft die Geschäftsdaten aus den E-Mail-Postfächern ausgespäht. Deswegen sollten alle Mitarbeiter regelmäßig geschult werden, niemals Kennwörter oder Bestätigungscodes für das E-Mail-Postfach auf Webseiten einzugeben, die sich nach dem Aktivieren von in E-Mails enthaltenen Links öffnen (**Phishing-Gefahr**).[2] Einige Betrüger kontaktieren die anvisierten E-Mail-Inhaber unter einer Legende (bspw. IT-Support oder Dienstleister) und verleiten **telefonisch**[3] zur Preisgabe von Bestätigungscodes oder zur Eingabe der Zugangsdaten auf einer Phishing-Webseite. Die erlangten Zugangsdaten verwenden die Betrüger zum Zugriff auf den betroffenen E-Mail-Account und zum Ausspähen sensibler Daten.

**Technische Prävention**

- Technische Maßnahmen werden von den IT-Fachkräften der Unternehmen oder durch beauftragte IT-Dienstleister geprüft, umgesetzt und eingerichtet.
- Sichern Sie unbedingt alle im Unternehmen verwendete E-Mail-Accounts mit einem **Zweiten Sicherheitsfaktor** (2FA oder auch MFA genannt).[4] Dies gilt auch für den Zugriff auf den E-Mail-Bereich durch Ihre Administratoren.
- **Prüfen Sie regelmäßig** unberechtigte Zugriffe auf E-Mail-Konten, E-Mail-Server oder auf das IT-Netzwerk. Unberechtigte Zugriffe können durch manuelle Prüfungen der Logfile- und Protokolldaten der E-Mail-Umgebung durch die IT-Fachebene festgestellt werden. Die automatisierte Erkennung abweichenden Verhaltens wird ebenfalls empfohlen. Prüfkriterien können sein:

[2] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Wie-erkenne-ich-Phishing-in-E-Mails-und-auf-Webseiten/wie-erkenne-ich-phishing-in-e-mails-und-auf-webseiten_node.html
[3] https://praevention.polizei-bw.de/wp-content/uploads/sites/20/2021/08/20210809-INFOBLATT-Vishing.pdf
[4] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html

  - Ungewöhnliche oder ausländische IP-Adressen,
  - Zugriffe außerhalb der regulären Arbeitszeiten (Nachtzeit, Wochenende),
  - Datenabflüsse (Rechnungsdokumente).
- Stellen Sie verdächtige Zugriffe fest, kontaktieren Sie unverzüglich den regulären Account-Inhaber der E-Mail-Adresse und gleichen Sie den Zugriff ab. Bestätigt Ihnen die Mitarbeiterin oder der Mitarbeiter, den Zugriff nicht vorgenommen zu haben, leiten Sie geeignete Sofortmaßnahmen ein (bspw. Account-Sperrung, Änderung Zugangskennwort, telefonische Information an die Geschäftspartner, Anzeige bei der Polizei).
- In diesem Fall sollten eventuell unbemerkt eingerichtete Weiterleitungs-E-Mail-Adressen in den Konfigurationseinstellungen des E-Mail-Accounts geprüft werden. Wird eine unautorisiert eingerichtete Weiterleitung festgestellt, sollte diese E-Mail-Adresse dokumentiert (Screenshot oder Notiz) und sofort gelöscht werden.
- Das im Unternehmen verwendete E-Mail-Programm sollte nicht nur den Namen des Absenders einer E-Mail, sondern auch die tatsächliche E-Mail-Adresse des Absenders anzeigen (**vollständige Darstellung der Absender-Informationen**).
- Die automatisierte Kennzeichnung externer E-Mail-Domains im Textbereich eingegangener E-Mails mit einer eindeutigen Formulierung für die Anwender stellt eine weitere empfehlenswerte Schutzmaßnahme dar.
- Weitere Möglichkeiten zur technischen Prävention bestehen in der technischen Absicherung des E-Mail-Servers zum Schutz vor „Spoofing“ (vorgetäuschte E-Mail-Absenderadressen).[5]

**Sofortmaßnahmen nach Feststellung eines Betrugsfalles**

- Greifen Sie auf die vorbereitete **Checkliste** zurück und arbeiten Sie die vorgegebenen Punkte ab.
- Festgestellte Zahlungsüberweisungen im betrügerischen Zusammenhang sollten so schnell als möglich der eigenen **Geschäftsbank** gemeldet werden mit der Bitte um Stornierung und Rückholung.

[5] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_mail_server_studie_pdf.pdf?__blob=publicationFile&v=1 (ab Punkt 5.2.2)

- Erstatten Sie so schnell als möglich Anzeige bei der **Polizei** (Kontaktdaten siehe unten). Die Polizei kann die behördlichen Maßnahmen zur Vermögenssicherung einleiten.
- Teilen Sie insbesondere die folgenden Punkte mit:
  - Datum der erfolgten Zahlungsüberweisung
  - Summe
  - Bankverbindung Zielkonto
  - Bankverbindung Abgangskonto
  - Leiten Sie die betrügerischen E-Mails weiter an die Polizei, wenn möglich als Anlage im Original.

**Zentrale Ansprechstelle Cybercrime (ZAC)**

Die ZAC dient als zentraler Ansprechpartner der Polizei für die Wirtschaft und Behörden von Baden-Württemberg in allen Belangen des Themenfeldes Cybercrime.


**Erreichbarkeit der ZAC Baden-Württemberg:**

**Telefon: +49 (0)711 5401 2444**
**E-Mail: cybercrime@polizei.bwl.de**

Erreichbarkeiten der Zentralen Ansprechstellen Cybercrime der Bundesländer:
www.polizei.de/zac