BEDROHUNGS-BIBLIOTHEK

JULITH GmbH
Awareness-as-a-Service

CEO-Fraud & Business Email Compromise (BEC)

BEC-Angriffe richten oft mehr Schaden an als Ransomware — und treffen Buchhaltung, Vorstandssekretariat, M&A-Teams. Wir zeigen, wie Angreifer Hierarchie ausnutzen und welche prozessualen Kontrollen wirklich helfen.

min Lesezeit: 8 min **Aktualisiert:** 14. März 2026 **Risiko:** Sehr hohes Risiko
Quelle: awareness-as-a-service.com/de/resources/threats/ceo-fraud

Was ist CEO-Fraud & BEC?

Business Email Compromise (BEC) bezeichnet Angriffe, bei denen Kriminelle E-Mail-Konten oder -Identitäten missbrauchen, um betrügerische Überweisungen, Datenabflüsse oder Vertragsmanipulationen zu erreichen. **CEO-Fraud** ist die bekannteste Variante: Eine gefälschte E-Mail scheinbar vom Geschäftsführer oder Vorstand fordert die Buchhaltung zu einer dringenden, vertraulichen Überweisung auf.

BEC ist laut FBI und ENISA seit Jahren die finanziell schädlichste Cyberkriminalität weltweit — nicht weil Einzeltaten so spektakulär sind, sondern weil so viele Unternehmen betroffen sind und die Schadenssummen pro Vorfall oft sechsstellig ausfallen. Technische Schutzmaßnahmen helfen wenig, wenn der Angriff keine Malware enthält und von einer legitim aussehenden Adresse kommt.

Die Angreifer recherchieren vorher: LinkedIn-Profile, Pressemitteilungen, Geschäftsberichte und Handelsregisterdaten liefern Organigramm, laufende Projekte und bevorstehende Transaktionen. Mit diesen Informationen klingen BEC-E-Mails täuschend echt.

Auf einen Blick

01

Kein Schadcode, kein Alarm

BEC-Mails enthalten weder Anhänge noch Links. Sie sehen aus wie normale Unternehmens-E-Mails — deshalb schlägt kein technisches System an.

02

Durchschnittlicher Schaden sechsstellig

Pro erfolgreichem BEC-Angriff entstehen im DACH-Raum im Schnitt Schäden im hohen fünf- bis niedrigen sechsstelligen Bereich. Rückbuchungen gelingen selten.

03

Hierarchie als Angriffsfläche

Die Kombination aus Autorität ("CEO") und Dringlichkeit ("sofort, vertraulich") schaltet kritisches Denken aus — unabhängig von Berufserfahrung oder Vorsicht.

Woran erkennen Sie CEO-Fraud & BEC?

Dringende Überweisung außer der Reihe
"Bitte veranlassen Sie noch heute EUR 85.000 auf folgendes Konto — wir sind mitten in einer vertraulichen Transaktion."

Geheimhaltungsgebot gegenüber Kollegen
"Das darf vorerst nicht im Team bekannt werden" oder "Bitte nicht über die üblichen Kanäle — direkt an mich." Prozess-Umgehung ist das stärkste Warnsignal.

Neue oder geänderte Bankverbindung
Lieferant oder Geschäftspartner gibt kurz vor Zahlung eine neue IBAN durch — oft kurz vor einer ohnehin anstehenden Überweisung.

Leicht abweichende Absender-Domain
CEO@firmenname-ag.com statt @firmenname.com, oder Tippfehler-Domain (firmennaem.com). Abweichungen sind oft nur ein Zeichen verschieden.

Ungewöhnliche Tageszeit oder Urlaubsabwesenheit
Angreifer timen Mails oft auf Freitagabend, Feiertagsbrücken oder wenn der vermeintliche Absender bekanntermaßen im Ausland ist.

Druck, interne Freigabeprozesse zu umgehen
"Das muss sofort raus, wir haben keine Zeit für das normale Prozedere" — jeder Versuch, das 4-Augen-Prinzip zu überspringen, ist ein Warnsignal.

So schützen Sie sich

Für Mitarbeitende

- **Nie Überweisungen aufgrund einer einzelnen E-Mail anweisen** — unabhängig davon, wer scheinbar der Absender ist.
- **Out-of-band-Verifikation:** Bei ungewöhnlichen Zahlungsanfragen immer telefonisch über eine bekannte Nummer bestätigen — nicht über eine in der Mail genannte Rückrufnummer.
- **Neue Bankverbindungen hinterfragen:** Änderungen an Lieferanten-IBANs immer über einen zweiten Kanal (Telefon, persönlich) bestätigen lassen.
- **Das Geheimhaltungsgebot ignorieren:** Kein legitimer Vorgesetzter schämt sich dafür, dass ein normaler Freigabeprozess eingehalten wird. Wenn jemand sagt "nicht mit Kollegen besprechen", ist das der stärkste Alarm.

Für Administratoren

- **4-Augen-Prinzip ab definiertem Schwellenwert** in der Buchhaltungs-Software erzwingen (z.B. ab EUR 5.000 zweite Freigabe erforderlich).
- **Stammdatenprozess für Lieferanten-IBANs:** Änderungen an Zahlungsverbindungen nur nach schriftlichem Antrag und Out-of-band-Bestätigung — nicht auf E-Mail-Basis.
- **DMARC** `p=reject` für alle Domains konfigurieren, um Domain-Spoofing zu erschweren.
- **Look-alike-Domain-Monitoring:** Dienste, die ähnliche Domains (Typosquatting) frühzeitig identifizieren.
- **BEC-Schulungsmodul** mit simulierten CEO-Fraud-Szenarien — Buchhaltung, Assistenz und Einkauf sind primäre Zielgruppen.

Echte Beispiele

FALL 01 · MASCHINENBAU-KMU · DE · Q4/2025

Die Assistentin des Geschäftsführers erhielt eine E-Mail scheinbar von ihrem Vorgesetzten, der sich auf einer Messe in Asien befand. Er bitte sie, EUR 230.000 an einen "M&A-Partner" zu überweisen — alles sei bereits mit dem CFO abgestimmt, aber bitte noch nichts kommunizieren. Die Assistentin überwies. Der echte Geschäftsführer war tatsächlich auf der Messe — dieser Umstand war LinkedIn zu entnehmen.

Schaden: EUR 230.000, davon EUR 60.000 zurückgebucht · **Erkennung:** CFO stellte drei Tage später eine Unregelmäßigkeit fest · **Lehre:** Out-of-band-Verifikation und ein klares "Geheimhaltungsgebot = Warnsignal"-Training hätten den Schaden verhindert.

FALL 02 · LOGISTIK-DIENSTLEISTER · CH · Q1/2026

Ein Lieferant informierte die Buchhaltung per E-Mail über eine neue IBAN für künftige Zahlungen. Die E-Mail wirkte authentisch — gleiche Absender-Domain, ähnliches Sprachbild. In Wirklichkeit hatte ein Angreifer das E-Mail-Konto des Lieferanten kompromittiert und wartete auf eine anstehende Zahlung. CHF 48.000 wurden auf ein Mule-Konto überwiesen.

Schaden: CHF 48.000, Rückbuchung gescheitert · **Erkennung:** Lieferant meldete sich wegen ausbleibender Zahlung · **Lehre:** IBAN-Änderungen immer telefonisch über bekannte Nummer beim Lieferanten bestätigen.

Was tun, wenn es passiert ist?

DIE ERSTEN 15 MINUTEN

1. **Bank sofort anrufen** (Sofortüberweisung-Stopp): Je schneller Sie reagieren, desto höher die Chance einer Rückbuchung. Minuten zählen.
2. **Transaktion dokumentieren:** Screenshot der E-Mail, Überweisungsbeleg, Zeitstempel — alle Belege sichern, nichts löschen.
3. **Geschäftsleitung und CFO informieren** — unabhängig davon, ob die Überweisung im Namen der Geschäftsleitung erfolgte.
4. **IT-Security / SOC:** Prüfen, ob ein Postfach kompromittiert wurde (bei "echter Domain, echter Absender").
5. **Strafanzeige:** Bei der Polizei und/oder Staatsanwaltschaft. In DE zusätzlich Meldung an das BSI, in CH an das NCSC.
6. **Lieferanten informieren,** wenn deren IBAN-Änderung Teil des Betrugs war — sie können ebenfalls Opfer sein.

Häufige Fragen

Hilft DMARC gegen CEO-Fraud?

Teilweise. DMARC verhindert exaktes Domain-Spoofing (ceo@ihrefirma.com). Es schützt nicht vor Look-alike-Domains (ceo@ihrefirma-ag.com) und nicht vor kompromittierten echten Konten. Es ist eine notwendige, aber keine hinreichende Maßnahme.

Warum erstatten Banken den Schaden nicht?

Eine autorisierte Überweisung — also eine, die Sie selbst in Auftrag gegeben haben, auch wenn aufgrund Täuschung — gilt rechtlich meist nicht als Bankfehler. Rückbuchungen gelingen nur, wenn das Zielkonto noch nicht leer ist. Das ist oft nicht der Fall.

Sind bestimmte Branchen besonders betroffen?

BEC trifft überproportional Unternehmen mit hohem Überweisungsvolumen, dezentralen Strukturen und häufigen Lieferantenwechseln: Bau, Logistik, Immobilien, M&A-aktive Konzerne und NPOs mit internationalen Transfers.

Was ist der Unterschied zwischen CEO-Fraud und BEC?

CEO-Fraud ist eine Unterform von BEC. BEC umfasst alle Varianten: gefälschte Rechnungen, IBAN-Manipulation, kompromittierte Postfächer, Lieferantenbetrug. CEO-Fraud meint speziell die Impersonation der Geschäftsleitung gegenüber Untergebenen.

Weitere Themen

CEO-Fraud ist die bekannteste Form des Social Engineerings im Unternehmenskontext. Wer BEC versteht, sollte auch die psychologischen Grundlagen des Social Engineerings und die Rolle von Insider Threats kennen.