Schützen Sie Ihr Unternehmen vor Zahlungs- und Fake-President-Betrug

Zahlungs- und Fake-President-Betrug sind eine zunehmende Bedrohung für Unternehmen weltweit.

Auf den folgenden Seiten erfahren Sie, wie Sie Ihr **Unternehmen effektiv schützen** können.

Seien Sie stets wachsam und hinterfragen Sie zweifelhafte Anweisungen.

Wichtige Informationen zu aktuellen Risiken

Was ist ein **Zahlungsbetrug?**

Bei Zahlungsbetrügen (Payment Diversion) geben sich Kriminelle als Mitarbeitende, Lieferanten oder Geschäftspartner Ihres Unternehmens aus und erreichen durch manipulierte Mitteilungen oder Rechnungen, dass die Bezahlung für erbrachte Dienstleistungen oder Waren auf abweichende Konten erfolgt (Umleitung von Zahlungsströmen / Bestellerbetrug).

Was ist ein **Fake-President-Betrug?**

Beim Fake-President-Betrug (auch CEO-Fraud genannt) handelt es sich um eine Form des Social Engineerings, bei der sich Kriminelle als Unternehmensführung ausgeben, um Mitarbeiter zu betrügerischen Überweisungen oder zur Herausgabe vertraulicher Informationen zu bewegen. Künstliche Intelligenz (KI) verstärkt dieses Risiko, indem sie realistische gefälschte Identitäten und Nachrichten erzeugt, die schwer zu erkennen sind. KI kann Schreibstile, Stimmen und sogar Videos (Deep Fakes) nachahmen, was die Täuschung glaubwürdiger macht.

Wie erkenne ich mögliche **Warnsignale?**

- Ungewöhnliche oder unerwartete Anfragen von Führungskräften
- Vermeintlich dringende oder vertrauliche Anweisungen
- Aufforderungen zur Umgehung standardisierter Verfahren oder von Sicherheitsprotokollen
- Änderungen von Kontoverbindungen der Mitarbeitenden, Dienstleister oder Geschäftspartner

Für weitere Informationen kontaktieren Sie uns unter

So verhindern Sie Betrugsversuche

Kommunikationsrichtlinien festlegen

Anweisungen per E-Mail, PDF, Brief, Fax erst nach telefonischer Bestätigung freigeben, da sie leicht gefälscht werden können. Nutzen Sie zur Verifizierung bekannte Rufnummern, nicht neu mitgeteilte.

Fälschungen erkennen

Achten Sie auf bekannte Floskeln wie „Hallo Lieblings-kollegin!“ und seien Sie sich bewusst, dass Fotos, Stimmen- und Video-Aufnahmen gefälscht werden können, auch durch KI.

Wachsamkeit bei Zeitdruck

Seien Sie besonders wachsam bei Zeitdruck, z. B. „Diese Zahlung muss bis heute Abend rausgehen!“

Vier-Augen-Prinzip anwenden

Zahlungsanweisungen nur im Vier-Augen-Prinzip freigeben (eine Stelle legt an, eine andere prüft und gibt frei).

Kommunikationskanal prüfen

Mails von @gmail.com, @gmx.de etc. sind keine typischen Geschäftsmailadressen. Überprüfen Sie die Absenderadresse genau. Änderungen von Konto-nummern, Lieferanschriften, Telefonnummern etc. sollten immer über etablierte Kommunikationskanäle verifiziert werden.

Sie möchten mehr erfahren?
Kontaktieren Sie uns für eine erste unverbindliche Beratung unter

Zurich Gruppe Deutschland
Platz der Einheit 2
60327 Frankfurt am Main
www.zurich.de

212811424 2504

ZURICH