CEO/BUSINESS E-MAIL BETRUG (CEO-BETRUG)

CEO-Betrug tritt auf, wenn ein Mitarbeiter, der zur Ausführung von Zahlungen berechtigt ist, dazu verleitet wird, eine gefälschte Rechnung zu bezahlen oder eine nicht autorisierte Transaktion von einem Geschäftskonto vorzunehmen.

WIE FUNKTIONIERT ES?

Die Betrüger, die sich als hochrangige Personen des Unternehmens (z.B. CEO oder CFO) ausgeben, rufen an oder schreiben eine E-Mail.

Sie verfügen über gute Kenntnisse über die Organisation.

Sie verlangen eine dringende Zahlung.

Sie benutzen Begriffe wie: 'Vertraulich', 'Die Firma vertraut Ihnen', 'Ich bin momentan nicht verfügbar'.

Es handelt sich oftmals um internationale Zahlungen, die an Banken ausserhalb Europas gehen.

Der Mitarbeiter transferiert Geld auf ein Konto, das durch den Betrüger kontrolliert wird.

Instruktionen bezüglich das weitere Vorgehen werden später über eine Drittperson oder über E-Mail bekanntgegeben.

Der Mitarbeiter wird angehalten, den regulären Autorisierungsprozess zu umgehen.

Sie nehmen Bezug auf eine sensible Situation (z.B. Steuerprüfung, Fusion, Akquisition).

WAS SIND DIE ANZEICHEN?

- Ungewöhnliche(r) E-Mail/Telefonanruf
- Direkter Kontakt zu einer leitenden Person, mit der Sie normalerweise nicht in Kontakt stehen
- Bitte um absolute Vertraulichkeit
- Druck und ein Gefühl der Dringlichkeit
- Ungewöhnliche Anfrage in Widerspruch zu internen Verfahren.
- Drohungen oder ungewöhnliche Schmeicheleien/Belohnungsversprechen

WAS KÖNNEN SIE TUN?

ALS UNTERNEHMEN

Nehmen Sie die Risiken ernst und stellen Sie sicher, dass **die Mitarbeiter ebenfalls informiert und sensibilisiert sind.**

Bestärken Sie Ihre Mitarbeiter, **Zahlungsanfragen mit Vorsicht zu behandeln.**

Implementieren Sie interne Prozesse für Zahlungen.

Implementieren Sie ein Verfahren zur Überprüfung der Rechtmässigkeit von Zahlungsaufträgen, die per E-Mail eingehen.

Implementieren Sie **Meldeverfahren bei Verdacht** auf CEO-Betrug.

Überprüfen Sie die auf Ihrer Unternehmenswebseite veröffentlichten Informationen, **schränken Sie diese ein und zeigen Sie Vorsicht** in Bezug auf soziale Medien.

Führen Sie technische **Sicherheitsupdates und -upgrades durch.**

Kontaktieren Sie bei Betrugsversuchen immer die Polizei, auch wenn Sie kein Opfer des Betrugs wurden.

ALS MITARBEITER

Halten Sie sich strikt an die Sicherheitsverfahren für Zahlungen und Beschaffungen. **Überspringen Sie keine Schritte und geben Sie bei Druck nicht nach.**

Überprüfen Sie immer die E-Mail Adressen, wenn Sie sensible Daten oder Geldüberweisungen verarbeiten.

Bei Zweifeln an einer Zahlung, **fragen Sie den zuständigen Kollegen.**

Öffnen Sie nie verdächtige Links oder Anhänge, die Sie über E-Mail erhalten. Seien Sie besonders vorsichtig, wenn Sie Ihre privaten E-Mails auf dem Geschäftscomputer abrufen.

Beschränken Sie Informationen und sind vorsichtig in Bezug auf soziale Medien.

Vermeiden Sie es, Informationen über die Hierarchie, Sicherheit oder Verfahren der Firma zu teilen.

Wenn Sie eine verdächtige E-Mail oder einen verdächtigen Anruf erhalten, informieren Sie immer Ihre IT-Abteilung.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

LIECHTENSTEIN BANKERS ASSOCIATION

#CyberScams