bankenverband

Blog

Cyberkriminalität: Risiko am Arbeitsplatz

10.10.2019

von

Altmann, Kathleen

Schlagworte

Verbraucher
Cybersicherheit
Cyberkriminalität

Unternehmen sind für Cyberkriminelle ein attraktives Ziel. Die Firmen werden über das Internet ausspioniert und Mitarbeiter von Kriminellen häufig gezielt ins Visier genommen. Selbst für

erfahrene Kollegen ist es schwierig, die Betrugsmaschen zu durchschauen. Diese Kniffe reichen von irreführenden Telefonanrufen bis hin zu E-Mails, die Mitarbeiter dazu bringen sollen, bestimmte Handlungen auszuführen oder Informationen preiszugeben.

Unternehmen im Visier: CEO-Fraud

Beim sogenannten Chef-Betrug („CEO-Fraud“) fordert der vermeintliche Chef einen zahlungsberechtigten Mitarbeiter per E-Mail auf, einen hohen Betrag an ein von ihm bestimmtes Konto anzuweisen und den Vorgang streng vertraulich zu behandeln. Es sind aber auch Fälle bekannt, in denen die Stimme des Unternehmenschefs imitiert wird. Hierbei bedienen sich Kriminelle einer Stimmimitationssoftware. Der Tonfall und die Sprechweise des vermeintlichen CEOs werden am Telefon nachgeahmt. Auch hier wird der betreffende Mitarbeiter unter Druck gesetzt, die angeblich dringende Finanztransaktion unter größter Geheimhaltung durchzuführen.

Wir beantworten alle Fragen rund um das Thema in unserem Lexikon Cyberkriminalität - und geben weitere Tipps, wie Sie sich schützen können.

Auch bei Geschäftsbeziehungen werden Tricks angewandt: So bedienen sich Kriminelle des Namens eines Geschäftspartners, um auf diese Weise rechtmäßige Zahlungen umzuleiten. Hierzu wird eine angeblich geänderte Bankverbindung mitgeteilt. Weitere Betrugsmaschen sind gefälschte Rechnungen von existierenden Geschäftspartnern. In Bezug auf den Inhalt und die Leistung können diese durchaus einer erwarteten Rechnung entsprechen. Die finanziellen Schäden bei diesen Betrugsmaschen sind oftmals hoch, ohne dass sich der handelnde Mitarbeiter eines Betruges überhaupt bewusst wird.

So können Unternehmen sich gegen Cyberkriminalität schützen

Gänzlich kann man es als Unternehmen wohl nicht verhindern, Opfer solcher Betrugsszenarien zu werden. Aber die nachfolgenden Tipps können dabei helfen, das Risiko zu minimieren.

Offene Unternehmenskultur fördern: In einer offenen Unternehmenskultur können Betrugsversuche schneller aufgedeckt und verhindert werden. Bei ungewöhnlichen Geschäftsvorfällen sollten Rückfragen bis in die Führungsetage möglich sein.

Auch Verbraucher geraten ins Visier von Cyberkriminellen. Hier erklären wir, wie Sie sich vor Phishing schützen

Risikobehaftete Prozesse prüfen: Welche Stelle könnte ein Einfallstor für diese Betrugsversuche sein? Nicht erst die Zahlungseingabe oder -freigabe sind kritisch. Bereits die Stammdatenänderungen, wie Kontoverbindungen oder Versan-

dadressen, können über gezielte Kontrollen oder festgelegte Prozesse abgesichert werden (auch bei Gehältern).

Mitarbeiter sensibilisieren: Es hilft zudem, Mitarbeiter über die gängigen Betrugsszenarien zu informieren. Auch beim Öffnen von E-Mails sollte man immer Vorsicht walten lassen. Es hilft, bei der E-Mail-Adresse zu prüfen, ob diese zum Absender passt und ob der Inhalt der Mail plausibel erscheint. Kontaktanfragen von Unbekannten über Social-Media-Netzwerke sollten nicht leichtfertig akzeptiert werden. Es braucht ein Bewusstsein aller Beteiligten dafür, dass die veröffentlichten Daten in solchen Netzwerken auch gegen die Person selbst genutzt werden können, zum Beispiel für einen Identitätsdiebstahl.

Nutzer- und Autorisierungsrechte überprüfen: Wichtig ist auch eine Überprüfung der Vergabe von Nutzerrechten. Diese sollten nur in dem Umfang vergeben werden, wie sie zur Erledigung der Aufgaben eines Mitarbeiters auch tatsächlich gebraucht werden. Bei der Vergabe von Autorisierungsrechten sollte als Minimalanforderung das Vier-Augen-Prinzip gelten – bei höheren Zahlungsbeträgen gegebenenfalls auch das Sechs-Augen-Prinzip. Auf die Vergabe von Einzelvollmachten sollte jedoch verzichtet werden.

Falls ein Betrugsfall eingetreten ist und kurzfristig erkannt wird, kann die kontoführende Bank helfen, wenn sie rechtzeitig informiert wird. Betrügerische Zahlungen können gestoppt werden, wenn sie dem Empfängerkonto noch nicht gutgeschrieben worden sind. In jedem Fall ist es auch bei einem abgewendeten Betrugsversuch wichtig, dass die Daten des Täterkontos der Bank und der Polizei mitgeteilt werden und Anzeige erstattet wird.