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

04.07.2022

Nahezu alle Unternehmen und Institutionen sind von Betrugsversuchen betroffen. Die Angreifer nutzen vielfältige Methoden, um die Betroffenen zur Überweisung von Geldern zu verleiten. Betrugsschaden im E-Mail-Verkehr ist vermeidbar. Die folgenden Empfehlungen tragen zur Abwehr von Betrugsversuchen bei und informieren über empfehlenswerte Sofortmaßnahmen beim Bekanntwerden eines E-Mail-Betrugs.

Wie gehen die Betrüger vor?

Sie greifen auf die E-Mail-Postfächer von Mitarbeiterinnen und Mitarbeitern der betroffenen Institutionen oder deren Geschäftspartner zu und spähen sensible Rechnungsdaten aus. Vorgefundene Rechnungsdokumente werden abgefangen und manipuliert. Die in der Rechnung angegebene **Bankverbindung wird verfälscht** und die manipulierte Rechnung an die Rechnungsempfänger weitergeleitet. Hierfür verwenden die Betrüger oftmals 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 Betrügern 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 Betrüger vor, die den Namen einer Mitarbeiterin oder eines Mitarbeiters im Unternehmen vortäuschen und der Personalstelle eine angeblich **geänderte Bankverbindung für die Gehaltszahlung** mitteilen.

Auch der „**falsche Geschäftsführer**“, der per E-Mail oder Messenger die Identität von Vorgesetzten vortäuscht und die Empfänger zu einer angeblich dringenden Überweisung oder zum Kauf von Gutscheinen zu verleiten versucht, tritt nach wie vor in Erscheinung.[1]

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

Sofortmaßnahmen nach Feststellung eines E-Mail-Betrugsfalles

- Greifen Sie auf die vorbereitete Checkliste zurück und arbeiten Sie die vorgegebenen Punkte ab.
- Festgestellte Zahlungsüberweisungen im betrügerischen Zusammenhang sollten schnellstmöglich der eigenen Geschäftsbank gemeldet werden mit der Bitte um Stornierung und Rückholung.
- Erstatten Sie anschließend schnellstmöglich Anzeige bei der Polizei. Die Polizei kann behördliche Maßnahmen zur Vermögenssicherung einleiten. Die Ansprechstelle der Polizei für Unternehmen und Behörden finden Sie auf der letzten Seite. Teilen Sie 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 E-Mail-Anlage im Original.

Sofortmaßnahmen bei unberechtigten Zugriffen auf E-Mail-Konten

- Unberechtigte Zugriffe können von der IT-Fachebene festgestellt werden. Prüfen Sie regelmäßig unberechtigte Zugriffe auf E-Mail-Konten, E-Mail-Server und IT-Netzwerk. Richten Sie automatisierte Prüfprozesse ein. Gewährleisten Sie auch regelmäßig manuelle Prüfungen der Protokolldaten der E-Mail-Umgebung. Beispiele für Prüfkriterien:
  - ungewöhnliche und ausländische IP-Adressen,
  - Zugriffe außerhalb der regulären Arbeitszeiten (Nachtzeit, Wochenende…),
  - Datenabflüsse (Rechnungsdokumente),
  - eingerichtete Filter- und Weiterleitungsregeln
  - Stellen Sie verdächtige Zugriffe fest, kontaktieren Sie unverzüglich den regulären Account-Inhaber der E-Mail-Adresse. Fragen Sie nicht per E-Mail, sondern telefonisch nach und gleichen Sie den Zugriff ab. Bestätigt Ihnen die Mitarbeiterin oder der Mitarbeiter, den Zugriff nicht selbst vorgenommen zu haben, leiten Sie geeignete Sofortmaßnahmen ein wie

  - Account-Sperrung und Änderung des Zugangskennwortes,
  - telefonische Information der Geschäftspartner,
  - Anzeige bei der Polizei (Kontaktdaten siehe letzte Seite).
- In diesem Fall sollten eventuell unbemerkt eingerichtete Weiterleitungsadressen und Filterregeln in den Konfigurationseinstellungen des E-Mail-Accounts geprüft werden. Stellen Sie unberechtigt eingerichtete Weiterleitungen fest, dokumentieren Sie die verdächtige E-Mail-Adresse mittels Screenshot oder Notiz für die Polizei und löschen Sie Weiterleitungsregel anschließend.

Organisatorische Prävention

- Bereiten Sie eine Checkliste mit den notwendigen Arbeitsschritten im Falle eines Betruges vor. Stellen Sie die Liste allen zuständigen Mitarbeiterinnen und Mitarbeitern auch in ausgedruckter Form zur Verfügung.
- Die Checkliste sollte
  - interne Zuständigkeiten (Geschäftsführung, Vorgesetzte, Rechnungsstelle, IT-Abteilung, Rechtsvertreter…) und
  - externe Zuständigkeiten (Hausbank, IT-Dienstleister, Polizei …)

  beinhalten sowie die jeweilige Erreichbarkeit.
- Betrügerische E-Mails werden zum Teil auch über die authentischen E-Mail-Adressen der Geschäftspartner oder der eigenen Vorgesetzten versandt. Verlassen Sie sich niemals auf die angezeigte Absender-E-Mail-Adresse. Prüfen Sie jede eingegangene E-Mail mit hoher Rechnungssumme eingehend.
- Definieren Sie betriebsintern eine kritische Summe für Rechnungsüberweisungen. Übersteigt eine eingegangene Rechnung diese Summe, sollte das angegebene Zielkonto beim Rechnungssteller unbedingt **telefonisch** oder mit einem Video-Anruf **verifiziert** werden. Gleichen Sie das angegebene Zielkonto gemeinsam mit Ihrem Geschäftspartner ab.
- Geht eine Nachricht mit der Mitteilung der angeblich **geänderten Bankverbindung** ein, sollte die angegebene Bankverbindung in jedem Fall wie empfohlen verifiziert werden.
- Kontaktieren Sie keinesfalls die in den Rechnungsdokumenten oder in E-Mails ersichtlichen Telefonnummern für die telefonische Verifizierung! 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 Telefonate mit den Rechnungsstellern auf das **eigene Adressverzeichnis** zurück.

- Die unbedingte Notwendigkeit der Verifizierung sollte allen Mitarbeiterinnen und Mitarbeitern, die berechtigt sind für

  - Auszahlungen,
  - Änderung von Stammdaten (Bankverbindung)

  als **verbindlicher Geschäftsprozess** vorgegeben werden.

- Dokumentieren Sie entsprechende Änderungsvornahmen der hinterlegten Stammdaten (Zeitpunkt, Veranlasser, verifiziert ja/nein, Name und Erreichbarkeit der bestätigenden Gegenseite, Angabe Verifizierungskanal, Ablage der eingegangenen Änderungsmitteilung…).
- Verzichten Sie auf beschleunigte Zahlungsmethoden wie Echtzeitüberweisung, Instant Payments oder CCU-Eilüberweisungen.

Verhaltensprävention für Mitarbeiterinnen und Mitarbeiter

Die Polizei empfiehlt regelmäßige Schulungen der zahlungsberechtigten Mitarbeiter. Empfehlenswerte Inhalte sind neben den erwähnten organisatorischen Prozessvorgaben insbesondere die betriebsinternen Meldewege zur Kontaktierung der Vorgesetzten oder der IT-Fachebene zur Mitteilung betrugsverdächtiger Beobachtungen (Checkliste). Weitere wichtige Schulungsinhalte betreffen die Phishing-Gefahr:[2]

- Zur Vorbereitung des Betruges werden oftmals die Rechnungsdaten aus E-Mail-Postfächern ausgespäht. Hierzu benötigen die Täter Zugriff auf E-Mail-Konten. Verpflichten Sie alle E-Mail-Anwender, niemals Kennwörter oder Bestätigungscodes für das E-Mail-Postfach auf Webseiten oder in Fenster einzugeben, die sich nach dem Aktivieren von in E-Mails oder in Office-/PDF-Dokumenten enthaltenen Links öffnen. Zum Einloggen in das E-Mail-Postfach zu verwenden sind ausschließlich die vorgegebenen Lesezeichen und Verknüpfungen.
- Erhalten Anwender Bestätigungsabfragen für den Zweiten Sicherheitsfaktor ohne eigene Veranlassung, ist dies ein konkretes Indiz für einen unberechtigten

[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

Zugriffsversuch. In diesem Fall wurde das Basis-Passwort bereits ausgespäht und wird verwendet. Beobachtungen dieser Art sind unverzüglich der IT-Fachebene zur Prüfung und Veranlassung von Sofortmaßnahmen zu melden.

- Einige Betrüger kontaktieren die anvisierten E-Mail-Inhaber unter einer Legende und verleiten telefonisch zur Preisgabe von Bestätigungscodes oder zur Eingabe der E-Mail-Zugangsdaten auf einer Phishing-Webseite. Die Anrufer täuschen die Zugehörigkeit zur IT-Abteilung oder zum IT-Dienstleister vor. Die erlangten Zugangsdaten verwenden die Betrüger zum unberechtigten Zugriff auf den betroffenen E-Mail-Account.
- Andere Anrufer täuschen vor, als Mitarbeiter der Geschäftsbank tätig zu sein und versuchen, TANs für Überweisungen oder Bestätigungscodes für das Online-Banking zu erfragen[3] oder versuchen, zur Eingabe dieser Daten auf einer bestimmten Webseite zu verleiten. Die Anrufer geben zutreffende Namen von tatsächlichen Bankmitarbeitern an und täuschen die dazugehörigen echten Telefonnummern vor. Ihre Bank erfragt niemals sensible Daten dieser Art!

Technische Prävention

Technische Gegenmaßnahmen 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 MFA genannt).[4] Dies gilt auch für den Zugriff auf den E-Mail-Bereich durch Ihre Administratoren.
- Richten Sie für alle Anwender verpflichtend zu verwendende Verknüpfungen oder Lesezeichen zum Einloggen in E-Mail-Postfächer ein.
- Konfigurieren Sie das im Unternehmen verwendete E-Mail-Programm in der Form, dass nicht nur der Name des Absenders einer E-Mail anzeigen wird, sondern auch die tatsächliche E-Mail-Adresse des Absenders (vollständige Darstellung der Absender-Informationen).
- Die technische Absicherung des E-Mail-Servers zum **Schutz vor „Spoofing“** (vorgetäuschte E-Mail-Absenderadresse) ist eine weitere elementare Schutzmaßnahme.[5]

[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
[5] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_mail_server_studie_pdf (ab Punkt 5.2.2)

- Aktivieren Sie im Alltag die möglichst umfangreiche, langfristige und manipulationssichere Protokollierung von Aktivitäten (Logfiles).
- Kennzeichnen Sie automatisiert externe E-Mail-Domains im Textbereich eingehender E-Mails mit einer eindeutigen Formulierung für die Anwender.
- Zur besseren Erkennbarkeit von Phishing-Webseiten sollten die im Unternehmen verwendeten Webbrowser im Bereich der Adresszeile standardmäßig den Domain-Namen einer URL betonen und die Subdomain und den Verzeichnispfad nicht oder weniger offensichtlich darstellen. Zur besseren Erkennbarkeit vorgetäuschter Domains und zur Erschwerung homographischer Angriffe sollten die Einstellung von Punycode im Browser immer „TRUE“ konfiguriert sein. Unterbinden Sie die Verwendung von IDNA und ähnlichen Funktionen im Browser.
- Prüfen Sie die Einrichtung moderner passwortloser Authentisierungsverfahren für Anwender. Das Verfahren kann zusätzlich zur 2FA eingesetzt werden.

Zentrale Ansprechstelle Cybercrime (ZAC)

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

Erreichbarkeit der ZAC Baden-Württemberg:

Telefon: 0711 - 5401 2444

E-Mail: cybercrime@polizei.bwl.de

Erreichbarkeiten der ZAC in den einzelnen Bundesländern: www.polizei.de/zac