Merkblatt zum Schutz und zum Umgang mit betrügerischen E-Mails im b2b-Handel

KRAFTFAHRZEUG GEWERBE

Herausgeber:
Deutsches Kraftfahrzeuggewerbe e. V.
Zentralverband (ZDK)
Franz-Lohe-Straße 21, 53129 Bonn

Markgrafenstraße 35
10117 Berlin

Telefon: 0228 9127-0
Telefax: 0228 9127-150
E-Mail: zdk@kfzgewerbe.de
Internet: www.kfzgewerbe.de

Verantwortlich:
Abteilung „Recht, Steuern, Tarife“
Rechtsanwalt Ulrich Dilchert / E-Mail: dilchert@kfzgewerbe.de

Verfasser:
Abteilung „Recht, Steuern, Tarife“
Rechtsanwalt Thomas Lehmacher / E-Mail: lehmacher@kfzgewerbe.de

Erscheinungsdatum: 09/2024

1 Problemlage

Insbesondere Automobilhändler sind oftmals Ziel betrügerischer E-Mails. Diese E-Mails enthalten in der Regel Angebote für Fahrzeuge mit unrealistisch hohen Rabatten und werden oft mit einem „Restpostenkatalog“ versendet. Strategie der Betrüger ist, Händler mit dem Ziel zu täuschen, diese zu einer Überweisung des Kaufpreises auf ihr Bankkonto zu veranlassen.

2 Vorgehensweise der Betrüger

Betrüger kompromittieren E-Mail-Postfächer von existierenden Betrieben (i.d.R. eine renommierte Händlergruppe). Sie nutzen dabei unzureichende Sicherheitsmaßnahmen der Händler im Hinblick auf die Sicherung ihrer E-Mail-Postfächer aus und wollen sowohl durch die Nutzung von Unternehmenskennzeichen als auch des Namens eines dort tätigen Mitarbeiters bei den angeschriebenen Autohändlern den Eindruck erwecken, als seien sie ein seriöser Verkäufer.

Sodann **senden die Betrüger E-Mails unter dem Namen des kompromittierten Händlers** an andere Händler und bieten darin Fahrzeuge zu stark reduzierten Preisen an. Die E-Mails enthalten oft einen Katalog mit angeblich sofort lieferbaren Lagerfahrzeugen. Reagiert ein Händler auf das Angebot, wird ihm die Verfügbarkeit des Fahrzeugs zugesichert und es werden ihm die Zahlungsmodalitäten (in der Regel Vorkasse) erläutert.

Es folgt eine **Rechnung im Stil des angeblichen Verkäufers** mit der Aufforderung, einen Zahlungsbeleg zur Bestätigung des Kaufvertrags zu übermitteln. **Nach der Überweisung des Kaufpreises bricht der Kontakt mit den Betrügern ab.** Die „gekauften“ Fahrzeuge werden dem Händler nicht geliefert.

3 Schutzmaßnahmen

E-Mail-Adresse auf verdächtige Elemente überprüfen

Vielfach werden die Absenderadressen von E-Mailadressen der kompromittierten Händler wie folgt manipuliert, um eine Identitätstäuschung beim Empfänger hervorzurufen:

- Manipulation des Namens vom vermeintlichen Absender vor dem @ in einer E-Mail:
  Anstelle des richtigen Nachnamens (z.B. lehm**ach**er@kfzgewerbe.de) wird ein ähnlich klingender Nachname (wie z.B. lehm**ah**er@kfzgewerbe.de) verwendet.

- Manipulation des Namens vom vermeintlichen Absender nach dem @ in einer E-Mail:
  Anstelle der richtigen „offiziellen“ Unternehmensdomain (z.B. lehmacher@kfzgewerbe.de) wird ein ähnlich klingender Nachname (wie z.B. lehmacher@kfzgewerbe**n**.de) verwendet.

Inhalt des Angebots kritisch prüfen

Der Händler ist gut beraten, skeptisch gegenüber besonders verlockenden Angeboten zu sein. Die angebotenen (vermeintlich günstigen) Konditionen sollten stets überprüft und mit dem (realistischeren) Marktpreis des jeweils angebotenen Fahrzeugs verglichen werden.

Nach Erhalt einer Rechnung

Angegebene Bankverbindungen sollten grundsätzlich mittels einer Zwei-Faktor-Authentisierung geprüft werden (z.B. durch einen Telefonanruf bei dem tatsächlichen Anbieter).

- Eine zu einer Verifizierung genutzte Telefonnummer sollte wegen der Gefahr der Manipulation nicht der Signatur von eingehenden E-Mails entnommen werden.
- Die zur Verifizierung verwendete Telefonnummer sollte dabei in der Regel eine dem Händler bereits bekannte Telefonnummer aus der eigenen Adressdatenbank sein oder vom Betrieb über die offiziellen Webseiten der als Absender aufgeführten Unternehmen entnommen werden.
- Von einer Verifizierung mittels einer einfachen E-Mail an seinen Ansprechpartner wird auf Grund des Risikos eines evtl. kompromittierten E-Mail-Postfachs dringend abgeraten.

Dokumentation und Meldung

- Bei Verdacht auf das Vorliegen eines kompromittierten E-Mail-Postfachs, sollte umgehend ein IT-Spezialist zum Zwecke der umfassenden Prüfung des konkreten E-Mail-Postfaches im Hinblick auf dessen betrügerische Verwendung durch Dritte und zum Zwecke der Dokumentation hinzugezogen werden.
- Sollte sich der Betrugsverdacht erhärten, ist eine Anzeige des Sachverhaltes bei der zuständigen Behörde zur Verhinderung weiterer Betrugsfälle dringend zu empfehlen.
- Für die Strafverfolgung und Bekämpfung von Cyberkriminalität sind in Deutschland zunächst die Polizeien der Bundesländer zuständig. Eine Übersicht zu spezialisierten Dienststellen, die insbesondere für Wirtschaftsunternehmen beratend und im Falle eines Cyber-Angriffs zur Verfügung stehen, kann hier abgerufen werden.

Interne Sensibilisierung

Händlern ist dringend zu empfehlen, regelmäßige Schulungen ihrer Mitarbeiter (insbesondere aus dem Bereich Verkauf) über aktuelle Betrugsmaschen durchzuführen, ihnen Informationsmaterialien zur Verfügung zu stellen und ihr Bewusstsein für solche kriminelle Aktivitäten zu schärfen (Sensibilisierung).


KRAFTFAHRZEUG
GEWERBE