(Foto: VRD - stock.adobe.com)

14.03.2024

Neue Betrugsfälle mit E-Mails: So schützen Sie Ihr Unternehmen

Aktuell bekommen Unternehmen wieder sogenannte Phishing-Mails. Deren kriminelle Absender wollen den Eindruck erwecken, die Mails stammten von der Industrie- und Handelskammer. Es handelt sich offenbar um eine Variation der bekannten Phishing-Kampagnen, vor denen bereits mehrfach gewarnt wurde. Ziel solcher Mails ist das Abgreifen von Daten.

Im aktuellen Fall ist in den Mails ein Link eingebettet. Die verlinkte Webseite bietet ein Formular an, mit welchem Informationen zu den Mitgliedsunternehmen gesammelt werden sollen. Dazu gehören die Anschrift des Unternehmens, Rufnummer und Kontoinformationen (IBAN). Wer solche verdächtige E-Mails erhält, sollte weder darin enthaltene Links noch Anhänge anklicken, sondern die Mail am besten löschen.

Die Polizeiliche Kriminalprävention der Länder und des Bundes gibt folgende **Tipps zum Schutz vor Phishing in Bezug auf Banken**.

- Vergewissern Sie sich, mit wem Sie es zu tun haben. Überprüfen Sie die Adressleiste in Ihrem Browser. Bei geringsten Abweichungen sollten Sie stutzig werden. Tragen Sie ständig benötigte Internet-Adressen in die Favoritenliste Ihres Browsers.
- Klicken Sie niemals auf den angegeben Link in der übersandten E-Mail. Versuchen Sie stattdessen, die in der E-Mail angegebenen Seiten über die Startseite Ihrer Bank zu erreichen (ohne diese in die Adresszeile einzutippen).
- Kreditinstitute fordern grundsätzlich keine vertraulichen Daten per E-Mail oder per Telefon oder per Post von Ihnen an. Wenn Sie sich unsicher sind, halten Sie in jedem Fall Rücksprache mit Ihrer Bank.
- Übermitteln Sie keine persönlichen oder vertraulichen Daten (bspw. Passwörter oder Transaktionsnummern) per E-Mail.
- Folgen Sie Aufforderungen in E-Mails, Programme herunterzuladen, nur dann, wenn Sie die entsprechende Datei auch auf der Internet-Seite des Unternehmens finden (Starten Sie keinen Download über den direkten Link). Öffnen Sie insbesondere keine angehängten Dateien. Nutzen Sie Antivirenprogramme und Firewalls.
- Geben Sie persönliche Daten nur bei gewohntem Ablauf innerhalb der Online-Banking-Anwendung Ihres Kreditinstituts an. Sollte Ihnen etwas merkwürdig vorkommen, beenden Sie die Verbindung und kontaktieren Sie Ihre Bank.
- Beenden Sie die Online-Sitzung bei Ihrer Bank, indem Sie sich abmelden. Schließen Sie nicht lediglich das Browserfenster und wechseln Sie vor Ihrer Abmeldung nicht auf eine andere Internetseite.

- Kontrollieren Sie regelmäßig Ihren Kontostand sowie Ihre Kontobewegungen. So können Sie schnell reagieren, falls ungewollte Aktionen stattgefunden haben.
- Pin und Tans sollten Sie nur dann eingeben, wenn eine gesicherte Verbindung mit Ihrem Browser hergestellt ist. Eine Sichere Verbindung erkennen Sie an dem https:// in der Adresszeile: Im Browserfenster erscheint ein kleines Icon, z. B. in Form eines Vorhängeschlosses, das den jeweiligen Sicherheitsstatus symbolisiert ("geschlossen" bzw. "geöffnet").
- Nutzen Sie nur die offizielle Zugangssoftware Ihrer Bank.
- Nutzen Sie Funktastaturen nur dann für das Online-Banking, wenn diese über eine eingebaute Verschlüsselung verfügen. Dies gilt auch für die Nutzung von Wireless-Lan (Wlan).
- Achten Sie auf einen Grundschutz Ihrer Hard- und Software.

ANSPRECHPARTNER

Presse und Kommunikation

MARCUS HORMES

Tel.: 0651 9777-122
Fax: 0651 9777-115
hormes@trier.ihk.de