DER OPTIMALE KOMPLETTSCHUTZ!

CYBER CRIME. VERSICHERUNG.
ARBEITSANWEISUNG FÜR DIE MIT ZAHLUNGSSTRÖMEN BEFASSTEN MITARBEITER.

ÖSTERREICH VERSION 8/2018

CYBER CRIME. ARBEITSANWEISUNG.

WICHTIGE HINWEISE FÜR DIE MIT ZAHLUNGSSTRÖMEN BEFASSTEN MITARBEITER

Die folgenden Informationen enthalten Arbeitsanweisungen zum Umgang mit Zahlungsanweisungen, Bankdaten, Kontoauszügen und Meldung von Auffälligkeiten / Betrugsversuchen:

1. EINZUHALTENDE ARBEITSANWEISUNGEN

Umgang mit Zahlungsanweisungen von Unternehmensleitern / Vorgesetzten

- Prüfung der Authentizität / Richtigkeit anhand von üblichen Anzeichen für Betrugsversuche (siehe Beispiele unter Ziff. 3) und
- Rückbestätigung unter Verwendung der üblichen bekannten Telefonnummern

Anfragen zur Verifizierung von Bankdaten / zum Erhalt von Informationen über Bankkonten, die von Bankangestellten kommen

- sind mit Unternehmensleitern / Vorgesetzten zu besprechen und
- Bestätigung der Authentizität solcher Anfragen unter Verwendung der bekannten Banktelefonnummer

Anweisungen zur Änderung von Bankdaten, die von Lieferanten oder Anbietern erteilt wurden

- Prüfung der Authentizität / Richtigkeit anhand von üblichen Anzeichen für Betrugsversuche (siehe Beispiele unter Ziff. 3) und
- Rückbestätigung unter Verwendung der bekannten Telefonnummern und
- Genehmigung durch einen Vorgesetzten

Kontoauszugsprüfung

- Nachweis zum Vieraugenprinzip bei Prüfung der Kontoauszüge

2. IM FALL EINES BEGRÜNDETEN VERDACHTS AUF EINEN BETRUGSVERSUCH

Per Telefon
Stellen Sie kritische Rückfragen zum Namen bzw. der Identität des Anrufers und vereinbaren Sie einen Rückruf zur vorherigen Absprache mit dem jeweiligen Vorgesetzten

Per Mail oder Post
Überprüfen Sie die Nachricht auf Authentizität / Richtigkeit anhand von üblichen Anzeichen für Betrugsversuche (siehe Beispiele unter Ziff. 3)

Weiteres Vorgehen

- Information an den jeweiligen Vorgesetzten oder IT-Sicherheitsbeauftragten, der über das weitere Vorgehen entscheidet
- Bei eindeutiger Identifizierung als Betrugsversuch und Löschung bzw. Abwehr durch den Mitarbeiter, ist der Vorfall trotzdem dem jeweiligen Vorgesetzten oder IT-Sicherheitsbeauftragten zu melden

CYBER CRIME. ARBEITSANWEISUNG.

WICHTIGE HINWEISE FÜR DIE MIT ZAHLUNGSSTRÖMEN BEFASSTEN MITARBEITER

3. AUFFÄLLIGKEITEN BZW. ANZEICHEN VON BETRUGSVERSUCHEN

Beispielhafte Anzeichen von Betrugsversuchen via Mail

- Die Absenderadressen scheinen gefälscht. Die Erkennung des gefälschten Absenders ist nur über die Header-Auswertung möglich.
- Die Anrede ist unpersönlich gehalten („Lieber Kunde der x-Bank!")
- Dringender Handlungsbedarf wird signalisiert oder Drohungen kommen zum Einsatz („Wenn Sie nicht sofort Ihre Daten aktualisieren, gehen diese verloren…" / „Wenn Sie das nicht tun, müssen wir Ihr Konto leider sperren…")
- Vertrauliche Daten (wie zum Beispiel PINs und TANs) werden abgefragt, etwa in einem Formular innerhalb der E-Mail.
- Die Mails enthalten Links oder Formulare, die vom Empfänger verfolgt beziehungsweise geöffnet werden sollen.
- Die Nachrichten sind in schlechtem Deutsch verfasst. Die Gründe dafür: Sie werden manchmal von Computerprogrammen aus anderen Sprachen automatisch übersetzt.
- Die E-Mails enthalten kyrillische Buchstaben oder falsch aufgelöste bzw. fehlende Umlaute (z. B. nur „a" statt „ä" beziehungsweise „ae").

Beispielhafte Anzeichen von Betrugsversuchen via Telefon oder Post

- IT-Administrator, der wegen eines Systemfehlers anruft, da er zur Fehlerbehebung noch das Passwort des Benutzers benötigt,
- Telefonentstörer, der einige technische Details wissen will, z. B. unter welcher Rufnummer ein Modem angeschlossen ist und welche Einstellungen es hat,
- Externer, der gerne Herrn X sprechen möchte, der aber nicht erreichbar ist. Die Information, dass Herr X drei Tage abwesend ist, sagt ihm auch gleichzeitig, dass der Account von Herrn X in dieser Zeit nicht benutzt wird, also unbeobachtet ist.
- Zahlungsanweisungen für Bußgelder o.ä. aus dem Ausland

Weitergehende Informationen finden Sie unter https://www.onlinesicherheit.gv.at

CYBER CRIME. ARBEITSANWEISUNG.

DIE NEUEN BETRUGSSZENARIEN DER ONLINE-GANGSTER

1. „FAKE PRESIDENT FRAUD“:
Durch die Vorspiegelung einer falschen Identität werden Zahlungen auf externe Konten angewiesen.

> *„Das Schreiben ist absolut vertraulich. Ich habe Sie ausgewählt wegen Ihrer Diskretion und Ihrer hervorragenden Leistungen, um für eine geplante streng vertrauliche Übernahme die damit verbundenen finanziellen Transaktionen auszuführen. Niemand außer Ihnen – auch nicht innerhalb unseres Hauses, ist derzeit über die Planungen informiert.“*

So oder ähnlich lautet häufig der Inhalt von E-Mails (oder selten auch Faxen) vom *„falschen Chef“*. Die Täter hacken sich ins Intranet und spähen dort meist über mehrere Tage Korrespondenzen aus, analysieren Duktus und Umgangsformen und fälschen dann den Mailaccount des Vorstandchefs. *„Fake President“* wird diese Masche deshalb auch genannt.

Bei dieser Betrugsmasche geben sich die Täter als ein Organ des versicherten Unternehmens – meist ein Vorstandsmitglied oder Geschäftsführer – aus und bitten per E-Mail oder Fax einen Mitarbeiter, der im Unternehmen für die Bankgeschäfte verantwortlich ist, eine dringende Überweisung auszuführen. Dem Mitarbeiter wird dabei vorgespiegelt, dass es sich um eine höchst geheime und vertrauliche Angelegenheit handelt, von der strategische Weichenstellungen im Unternehmen abhängen.

Häufig geht diese E-Mail mit Anweisungen an einen Mitarbeiter in der Buchhaltung in einer Tochtergesellschaft, da die Wahrscheinlichkeit höher ist, dass Mitarbeiter den obersten Chef nicht persönlich kennen. Distanz, Respekt und ein geschmeicheltes Ego erleichtern die Betrugsmasche in der Regel erheblich. Zudem wirft es weniger Fragen auf, wenn er den/die Mitarbeiter/in bittet, ihn weder persönlich noch telefonisch zu kontaktieren oder anzusprechen, nur per E-Mail. Die Begründungen für den E- Mail Verkehr sind teilweise absurd und gehen bis zur *„schriftlichen Dokumentation für Aufsichtsbehörden“*.

In vielen Fällen wird der Mitarbeiter gebeten, eine mit der Transaktion betraute Anwaltskanzlei zu kontaktieren, um das weitere Vorgehen detailliert zu besprechen. Der falsche Chef liefert die Kontaktdaten in seiner E-Mail mit. Der Kontakt in der angeblichen Kanzlei spricht in der Regel akzentfreies Deutsch und übt häufig erheblichen Druck auf die Mitarbeiter aus, was die strenge Geheimhaltung betrifft.

Die Betroffenen, die sich einerseits aufgrund des besonderen Vertrauens durch den Vorstand geschmeichelt fühlen, andererseits aufgrund der angeblichen Wichtigkeit der Transaktion erheblich unter Druck stehen, führen diese Überweisungen meist zügig aus. Fast immer erfolgen die Geldtransfers auf ausländische Konten, vor allem in Asien und Osteuropa. Fliegt der Betrug dann auf, sind die Konten dort meist leergeräumt oder eine Rückholung wird aufgrund des ausländischen Rechtssystems erheblich erschwert.

DIE NEUEN BETRUGSSZENARIEN DER ONLINE-GANGSTER

Neue Variante: FAKE IT SECURITY

Zuletzt ist vereinzelt eine neue Variation des Fake President Betrugs aufgetreten. Der Erstkontakt erfolgt wie in den bisher verbreiteten Betrugsfällen per E-Mail. Anschließend ruft jedoch ein *„falscher IT Security Mitarbeiter"* bei dem betreffenden Mitarbeiter an, um ihm mitzuteilen, dass bei ihm ein Fake President Betrugsversuch unternommen wurde, den man aber identifiziert habe. Da man die Täter aber auf frischer Tat ertappen wolle, solle der Mitarbeiter einfach *„weiter zum Schein mitspielen"* – auch zum Schein die Überweisungen / Finanztransaktionen tätigen. Vorstand und IT Security seien involviert und hätten entsprechende Vorsorgemaßnahmen getroffen, dass die Überweisung nur zum Schein getätigt wird und so abgesichert, dass kein finanzieller Schaden entstehen könne.

Da der Anrufer ein Betrüger ist, ist das Geld natürlich weg. Der weitere Verlauf der Betrugsfälle ist wie bei der klassischen Fake President Variante.

2. „PAYMENT DIVERSION FRAUD":
Betrug durch Umleitung von Zahlungsströmen, beispielsweise durch Vorspiegelung von angeblich neuen Kontodaten des Lieferanten.

In diesen Fällen hacken sich die Betrüger in die Server von Geschäftspartnern. Sie geben sich als Geschäftspartner oder Lieferant des versicherten Unternehmens aus und erreichen durch gefälschte E-Mail Mitteilungen, dass die Bezahlung für Waren oder erbrachte Dienstleistungen auf abweichende Konten erfolgt.

Die Umsetzung dieser Form des Betrugs wird ermöglicht durch ein gefälschtes Schreiben an das versicherte Unternehmen, dass sich die bisher vereinbarten Bankverbindungen geändert haben und der Zahlungsverkehr nun über die neue Bankverbindung abgewickelt werden soll. In diesem Schreiben sind auch Kontaktdaten angegeben und die Betrüger setzen darauf, dass der Mitarbeiter in der Buchhaltung zur Überprüfung der Echtheit der Mitteilung die dort aufgeführten gefälschten Telefonnummern nutzt.

Wird diese Änderung nicht mit den im firmeneigenen System registrierten Kontaktdaten telefonisch überprüft, ist das Geld in der Regel binnen weniger Stunden weg. Der Betrug fällt erst dann auf, wenn sich der Lieferant mit Mahnungen meldet, dass die Rechnung nicht fristgerecht bezahlt wurde.

3. „FAKE IDENTITY FRAUD":
Umleitung von Warenströmen an eine vermeintlich andere Lieferadresse des Kunden.

Bei diesem Betrugsszenario geben sich die Täter als ein bereits existierender Kunde oder als ein Neukunde des versicherten Unternehmens aus und ordern schriftlich Waren.

Mit plausiblen Erklärungen wird dann die Lieferung an eine abweichende Lieferadresse verlangt – ebenfalls per E-Mail nach vorherigem Identitätsdiebstahl.

Da die Identität einer tatsächlich existierenden Firma genutzt wird, schöpfen die Betrugsopfer zunächst keinen Verdacht. Oft fliegt der Betrug erst dann auf, wenn Zahlungsverzug eintritt und die tatsächlich existierende Firma gemahnt wird. Wird dann die Lieferadresse durch die Polizei überprüft, werden die Geschäftsräume verlassen vorgefunden und die Ware ist selbstverständlich längst weiter verschoben