1 Betrug durch Internet, Email und Telefon

Werden Sie oder Ihre Mitarbeiter angerufen oder auf anderem Wege kontaktiert, besteht immer die Möglichkeit, dass es sich dabei um Betrüger handelt. Die nachfolgenden Punkte sollen helfen, die Spreu vom Weizen zu trennen.
Aktuelle Änderungen an diesem Dokument sind mit einem roten Strich am rechten Rand gekennzeichnet.

1.1 Achten Sie auf Warnhinweise

- unerwartete Nachrichten (hinsichtlich Zeitpunkt, Urheber, Thematik, …)
- allzu verlockende Versprechungen, oder Hiobsbotschaften
- Aufforderung zum sofortigen Handeln
- Aufforderung zur Geheimhaltung
- Aufforderung zur Missachtung von Vorsichtsmaßnahmen, unabhängig ihrer Art
- Drohung mit gravierenden Konsequenzen, wenn Sie nicht kooperieren
- Fragen, deren Antwort einen Fremden nichts angeht (z.B. nach der Bankverbindung, Zählernummern, Passworten oder PINs)
- ZIP-Anhänge, wo z.B. wenige PDFs ausreichen würden
- Anhänge mit „komischen“ Endungen, z.B. „rechnung.pdf.html“ oder „rechnung.pdf.zip“

1.2 Das sollten Sie sofort tun

- Werden Sie sich bewusst, dass dies vermutlich ein Manipulationsversuch ist!
- Dann tief durchatmen, zurücklehnen, eine Tasse Kaffee (oder Tee) trinken und …
- die Nachricht nochmals in Ruhe kritisch prüfen.
- Ist dies nicht ohne weiteres möglich (z.B. werden Anrufer „einfach nicht locker“ lassen), ziehen Sie die **Notbremse** und brechen Sie den Kontakt hart ab:
  Legen Sie auf! Sperren Sie den Anrufer! Und halten Sie alle weiteren Kontaktversuche fern – nicht hinhören, nicht hinsehen! Wenn nötig, lassen Sie das Telefon liegen und gehen zum Nachbarn!
- Wenn Sie auch nach der Prüfung unsicher sind: nehmen Sie Kontakt mit dem vermeintlichen Absender auf, und verwenden Sie hierfür die Ihnen schon zuvor bekannten Wege – die altbekannte Telefonnummer, Email- oder Internetadresse. Nutzen Sie nicht die Rückruftaste und nicht die Antworten-Funktion.

1.3 Checkliste zur genaueren Prüfung

- Könnte jeder diese Nachricht, ohne Vorkenntnisse, als „Schuss ins Blaue“ gesendet haben?
- Erwarten Sie vom vermeintlichen Absender überhaupt Nachrichten dieser Art?
- Entspricht der Versandweg (Post, Mail, Portal-Download, WhatsApp, …) dem Üblichen?
- Sieht die Nachricht so aus, wie Sie sie vom vermeintlichen Absender erwarten würden?
  - Briefpapier und Layout
  - persönliche Anrede und Grußformel
  - Kontaktinformationen, wie z.B. Rückrufnummern
  - Referenzen, wie Ihre Kunden- oder Steuernummer
  - Formulierungen, Wortwahl, Satzbau, Rechtschreibung, …
  - Bei Zahlungsaufforderungen:
    Angaben zu den Zahlungsmodalitäten, bekannte IBAN und Verwendungszweck, „Rechnung“/„Gebührenbescheid“/„Steuerbescheid“
  - Format der Anhänge
- Auch wenn dies der Fall ist, und es handelt sich um eine Email oder ein PDF:
  - Passt der Email-Absender (siehe auch auf der nächsten Seite)?
    Lassen Sie sich den Absender vollständig anzeigen.
  - Passen die Links, die Sie aufrufen sollen, in der Nachricht?
    Fahren Sie mit der Maus über den Link, die Aufruf-URL wird dann unten im Browserfenster angezeigt. Achtung: der Tooltip direkt an der Maus ist Teil des Nachrichtentextes und entspricht im Zweifel nicht der URL!
  - Passen weitere Verweise, z.B. zum Kontaktformular oder Impressum? Bei Fälschungen sind diese häufig nur als Text dargestellt, ohne Link-Funktion.
  - Gibt es Links mit „http://…“? Stand der Technik sind gesicherte Verbindungen mit „https://…“

1.4 Die Tricks der Betrüger: so bleiben sie unerkannt

Die Betrüger geben sich möglicherweise als jemand anders aus, z.B. als Ihr Bekannter „Ulf Abt“ (ulf@abt.de).
Beispiele:

- **Email-Adresse:**
  Sie werden per Email angeschrieben. Dabei wird zwar der korrekte Name „Ulf Abt“ angezeigt, die Antwort geht jedoch an eine fremde Emailadresse, wie „info@bell038.b2bedge.de“ oder „ulf@abt.be“. Achtung: auch wenn die Emailadresse korrekt ist, kann es sich um einen Betrug handeln!
- **Email-**Adresse:
  Sie werden per Email angeschrieben, von Ihrer eigenen Emailadresse als Absender. Dies bezweckt, dass Sie diese Emailadresse als „bekannt“ ignorieren, obwohl sie dort nicht angebracht ist.
- **Briefpost:**
  Sie werden mit einem Brief auf Papier angeschrieben. Der Inhalt, einschließlich der Absenderdaten, kann frei erfunden oder echten Formularen nachempfunden sein. Vermeiden Sie Unterschriften, Bestätigungen oder Zahlungen ohne detaillierte Prüfung!
- **QR-Codes:**
  Sie erhalten eine Mailadresse oder URL in Form eines QR-Codes. Auch die so dargestellte Adresse kann, wenn aufgerufen, einer regulären Adresse täuschend ähnlich sehen (z.B. „https://www.abt.be“). Besonders gefährdet sind öffentliche Aushänge, die überklebt werden können (bei Plakaten, Ladesäulen, Bikesharing, für Wifi-Verbindungen, PayPal-Konten, …).
- **Telefonanrufe:**
  Sie erhalten einen Anruf von einer Ihnen bekannten Telefonnummer, z.B. der 110 oder von einem Geschäftspartner. Seien Sie sich bewusst, dass es technisch möglich ist, die dargestellte Telefonnummer zu manipulieren. Die Polizei wird Sie nie über die Notrufnummer 110 anrufen!
- **Kontoverbindung:**
  Sie erhalten eine Zahlungsaufforderung mit einer Kontoverbindung. Wenn Sie eine Überweisung dorthin tätigen, wird diese im Zweifel auch dann ausgeführt, wenn der Name des Empfänger-Kontoinhabers nicht der Angabe in Ihrer Überweisung entspricht.
- **Bargeld, Gutscheine und Kryptowährungen:**
  Solche Zahlungswege sind per se nicht nachvollziehbar und sollten nur mit Vorsicht und im Rahmen persönlicher Treffen, von Angesicht zu Angesicht, genutzt werden.
- **Internet- und Emailadressen** muss man „von rechts nach links“ lesen, relevant ist der Teil ab dem vorletzten Punkt. Betrüger fügen möglicherweise bekannte Adressteile vorne hinzu.
  Beispiele für Internet-Dienste von Silke Katz Steuerberaterin:
  - https://www.**katz-stb.de**
  - https://karriere.**katz-stb.de**
  - mail@**katz-stb.de**

  Auf folgende Internetseiten und Emails hat die Kanzlei keinen Zugriff, auch wenn die Adressen täuschend echt aussehen können:
  - https://katz-stb.**karriere.de**
  - https://**karriere-katz-stb.de**
  - https://www.**katz_stb.de**
  - https://www.**katz-stb.be**
  - mail@katz-stb.**karriere.de**
  - mail@**katz-stb.be**

1.5 Praxisbeispiele

Email-Absender:

- Jörg Schur von IONOS <jorg.schur@service.ionos.de> <info@**outfit-bi.de**>
- ADAC KartenService <adac-germany@shell.**domeneshop.no**>
- Porsche AG <noreply@porsche.**de-my.info**>
- Bei Werbe-Emails wird teilweise auch die Email des Empfängers als Absender eingetragen.

Links:

- In einer Email der Deutschen Bank:
  https://**bjcoachingaffaires.ca**/a5s65a125de1515ed.php
- In einer Email von Bitpanda.com:
  http://bitpanda.**013009.com**/
- Emails allgemein:
  basieren diese auf manipulierten Kopien von Original-Emails, werden Links z.B. zum Impressum oder zum Kundenportal häufig durch reinen Text ersetzt, und eingebettete Bilder gehen verloren.

2 Betrugsmaschen

Betrüger gehen oftmals in mehreren Schritten vor; dabei nutzen sie Informationen, die sie zuvor erhalten haben, und ein entsprechendes Auftreten (Small Talk, Fachjargon, Drohungen und Versprechungen jeglicher Art) um sich über einen anderen Weg Vertrauen, Autorität und weitergehende Informationen zu erschleichen - „Social Engineering“. Es ist ein Puzzle, bei dem auch kleine Teile bedeutsam werden können.

Die nachfolgend dargestellten Punkte und Beispiele sind nicht abschließend:

2.1 Ziele der Betrüger

Zur Vorbereitung:

- Von Interesse sind Informationen über das Unternehmen, seine Strukturen und Arbeitsabläufe.
- Ein Anrufer bittet um Informationen, die man zwar als unkritisch erachtet, die aber trotzdem nicht öffentlich bekannt sind.
- Per Email oder Fax sendet ein vermeintlicher Geschäftspartner neue Emailadressen, Faxnummern o.ä., um Kommunikationswege umzuleiten.
- Ein „Administrator“ erfragt Passwörter für den Abschluss wichtiger Arbeiten.
- Der Mitarbeiter wird dazu gebracht, ein Programm oder eine Internetseite aufzurufen, das Schaden verursacht, fremden Zugriff auf das Netzwerk ermöglicht, oder vertrauliche Informationen offenlegt.
- Im privaten Bereich kann ein Betrüger (bzw. eine Gruppe dahinter) über ein Dating-Portal eine Fernbeziehung zu einem Opfer aufbauen und vertiefen.

Das Finale:

- Der „Geschäftsführer“ eines Unternehmens veranlasst eine größere Finanztransaktion, die im Vorfeld streng vertraulich bleiben muss.
- Rechnungen werden von „Geschäftspartnern“ an die korrekte Rechnungsadresse gesendet, jedoch mit manipulierten Zahlungswegen.
- Eine manipulierte Telefonanlage initiiert Verbindungen zu kostenpflichtigen Mehrwertdiensten oder zu Auslandsnummern, an deren Erlösen die Betrüger beteiligt sind.
- Die Betrüger drohen mit der Veröffentlichung vertraulicher Informationen und erpressen damit Schweigegeld.
- Die Betrüger legen Computersysteme und damit die Produktion lahm und erpressen damit Lösegeld.
- Im privaten Bereich bittet ein vermeintlicher Verwandter, Bekannter oder eine Autoritätsperson (Polizist, Staatsanwalt, Notar, …) um Geld oder Wertsachen, sei es wegen eines Notfalls (Krankheit, Kaution, Räuber in der Nachbarschaft) oder eines Geschäfts (z.B. Hauskauf).

2.2 „Schuss ins Blaue“

per SMS:

- „Hallo Mama. Schick mir eine Nachricht auf WhatsApp (015…), mein altes Handy ist kaputt. Alte Nummer kannst du löschen.“ – anschließend folgt die Bitte um Geld wegen eines Notfalls

per Email:

- „Letzte Erinnerung – Bestätigung Ihrer Kundendaten erforderlich“ – mit Link, vermutlich zum Abgreifen der Zugangs-Daten
- „Ich habe Ihre Geräte gehackt und vollen Zugriff auf Bildschirm, Kamera und Mikro. Wenn Sie nicht … Bitcoins bezahlen, sende ich all Ihren Kontakten Aufnahmen, wie Sie Erwachsenen-Videos ansehen …“

per Telefonanruf, ohne Rufnummernübermittlung:

- „Hallo, dies ist Paypal. Ihr Einkauf in Höhe von 566,- € wurde als verdächtig eingestuft und wird zurückgestellt. Bitte drücken Sie sofort die 1, um mit einem Kundenbetreuer zu sprechen“

2.3 „Zu schön um wahr zu sein“

- „Wussten Sie, dass Sie jeden Tag ganz einfach rund 250 Euro verdienen können?“ – mit Link zu einer Plattform für die automatische Geldgenerierung durch Kryptowährungen. Eine solche Plattform wird jedoch faktisch immer eine Investition erfordern.
  Ist die Plattform eine Fälschung, dann ist das Geld verloren, „Gewinne“ und „vorübergehende Kurseinbrüche“ sind nur fiktiv und sollen zu weiteren Investitionen verleiten.
  Ist die Plattform real, sind Einlage und Gewinn sind nicht garantiert und der Handel hoch spekulativ.
- „2000,-€ Nebenverdienst mit 1 Std./Tag“ – häufig in Form von Geldtransfer über das eigene Konto, d.h. man wird wegen Geldwäsche zum Mittäter.

- „5.373.051,00 € Spende“ / „Ihre E-Mail-Adresse wurde zufällig … ausgewählt. … Bitte antworten Sie auf diese E-Mail, um weitere Informationen zu erhalten.“
- „Herzlichen Glückwunsch! Sie wurden als einer der Gewinner von 5.500.000 USD … ausgewählt.“