Wie Cyberkriminelle Unternehmen und Händler um Geld prellen

Mit fingierten Rechnungen oder Bestellungen wollen Internetbetrüger Unternehmen und Onlineshops übers Ohr hauen. Der Schaden geht schnell in die Zehntausende. Doch die Betroffenen können mit guten Prozessstrukturen und überlegter Kommunikation vorbeugen.

Von Markus Montz

kompakt

- Cyberkriminelle versuchen, Unternehmensbuchhaltungen mit fingierten Zahlungsanweisungen aus der Chefetage hinters Licht zu führen.
- In einer Variante täuschen sie Änderungen von Kontoverbindungen vor. Onlinehändler wollen sie durch fehlerhafte Rückabwicklungen von Lastschriften abzocken.
- Gegen die Maschen hilft, die Angriffsfläche durch gute interne Strukturen zu verringern sowie alle Mitarbeiter über die Methoden aufzuklären.

Der Absender klingt vertraut, der Mailinhalt plausibel: Wegen eines kurzfristigen Beschlusses von ganz oben solle die Buchhaltung schnell einen höheren Betrag überweisen, damit ein gerade eingefädelter Deal nicht platzt. Doch was nach Post aus der Geschäftsleitung oder vom langjährigen Geschäftspartner aussieht, soll Buchhaltungen und manchmal sogar die Unternehmensinhaber dazu verleiten, Geld an ein Konto von Betrügern zu schicken – wo es dann meist auf Nimmerwiedersehen verschwindet.

An anderer Stelle sind derzeit Händler betroffen. Sie

reagieren redlich und seriös auf Stornierungen, überweisen per Lastschrift eingegangenes Geld zurück und sehen sich plötzlich mit hohen Verlusten konfrontiert. Wir stellen drei Maschen vor, die sich gegen Unternehmen und Händler richten und von denen uns Leser berichtet haben. Dazu geben wir Tipps, wie sich die betroffenen Mitarbeiter, aber auch Unternehmensführungen oder Inhaber von Kleinunternehmen präventiv gegen die Betrugsversuche wappnen können – und wie sie den Tätern das Leben zumindest ein wenig schwerer machen können, wenn sie hereingefallen sind.

CEO-Betrug

Frieda K. arbeitet in der Kreditorenbuchhaltung eines mittelständischen Unternehmens. In ihren Aufgabenbereich fällt, das Geld für offene Rechnungen an Empfänger auf der ganzen Welt zu überweisen. An einem Freitagnachmittag erhält sie eine überraschende Mail, scheinbar direkt aus der Geschäftsführung: Sie solle noch vor dem Wochenende einen mittleren fünfstelligen Betrag an einen neuen Geschäftspartner überweisen. Die Sache sei eilig und Frieda K. müsse den Vorgang unbedingt vertraulich behandeln. Andernfalls könne ein wichtiges Erweiterungsprojekt des Betriebes platzen.

Die in Wahrheit nicht aus ihrem Unternehmen stammende Mail ist namentlich an Frieda K. adressiert und gibt als Absendernamen die Geschäftsführerin an. Auch die Anrede ist an Frieda K. gerichtet, weitere Empfänger gibt es nicht. Der Text ist knapp, aber fehlerfrei. Der Verwendungszweck klingt plausibel, es geht um die Anschaffung von Maschinen. Das Konto befindet sich zwar ebenso wie der Geschäftspartner in der Volksrepublik China. Es wäre jedoch nicht das erste Mal, dass Rechnungen von dort kommen und Überweisungen dorthin gehen.

Betreff: AW: Anfrage: 14/10/2021
Von:
Datum: 14.10.2021, 12:04
An: @ .de>
Kopie (CC):

Okay.

Ich werde sicherstellen, dass Sie die Rechnung so schnell wie möglich erhalten.

Die Zahlung erfolgt für den Kauf von Werkzeugen, Ausrüstungen und anderer Logistik.

Bankname: Sparkasse Aachen
IBAN: DE89
BIC: AACSDE33XXX
Bankadresse: Friedrich-Wilhelm-Platz 1 - 4 52062 Aachen, Deutschland

Name: AG
Empfängeradresse: Deutschland
Betrag: 2.693,85 EUR

Referenz:
Rechnungnummer:

Die Rechnung hierfür wird mit den gelieferten Materialien versendet.

Schick mir bitte eine Kopie der Zahlungsbestätigung per E-Mail, wenn du fertig bist

LG

Die Betrüger geben sich als Geschäftsleitung aus und schicken der Buchhaltung eine vorgetäuschte Zahlungsanweisung.
Auf die Freigabe durch ihren direkten Vorgesetzten und das übliche Vier-Augen-Prinzip solle sie ausnahmsweise verzichten, schreibt die vorgebliche Geschäftsführerin noch. Man werde ihre Mithilfe aber bei der nächsten Gehaltsrunde berücksichtigen. Bei Rückfragen solle Frieda K. ihr auf die Mail antworten, da sie wegen einer Dienstreise telefonisch nicht erreichbar sei.

Frieda K. hat die Daten bereits in eine Überweisungsvorlage eingegeben, da wird sie misstrauisch. Sie greift zum Telefon und ruft ihren Chef an. Nach einer halben Stunde folgt die Rückmeldung: Sie solle die Überweisung auf keinen Fall ausführen und die Mail an die IT-Sicherheit weiterleiten. Die echte Geschäftsführerin sei aus allen Wolken gefallen. Die Mail müsse eine hervorragend gemachte Fälschung sein. Das

vermeintliche Projekt gebe es ebenso wenig wie den chinesischen Geschäftspartner.

Gezielte Angriffe

Nicht immer handeln die Mitwirkenden so umsichtig wie in unserem Beispiel. Mitunter haben die Täter mit diesem „CEO-Betrug“ Erfolg. In zwei spektakulären Fällen haben ein deutsches und ein österreichisches mittelständisches Unternehmen vor einigen Jahren jeweils zweistellige Millionenbeträge verloren.

Der Name der Betrugsmasche leitet sich von der englischen Abkürzung CEO für „Chief Executive Officer“ ab. Dieser im englischsprachigen Raum verbreitete Titel entspricht in etwa einem Geschäftsführer oder Vorstandsvorsitzenden.

Die Masche trifft nicht nur Unternehmen. Polizeibehörden warnen vor ähnlichen Mails, die an Vereine aus Sport, Wirtschaft und Gesellschaft gehen, ebenso an Hochschulen und andere Bildungsträger. Den Ausgangspunkt bildet stets ein handwerklich gut gemachtes Social Engineering. Das bedeutet, dass beim eigentlichen Angriff niemand in die Firmensysteme eindringt, sondern dass die Täter ihre Opfer psychologisch raffiniert zu selbstschädigendem Verhalten verleiten – während diese glauben, das Richtige zu tun.

Dabei suchen sich die Täter ihre Opfer bewusst aus. Sie verfügen über Detailinformationen zum Unternehmen und kennen häufig auch die interne Aufgabenverteilung. Die Täter verschicken mit diesem Wissen gezielte Phishingmails an relevante Personen, in selteneren Fällen rufen sie auch an oder nutzen die Briefpost – präzise wie mit einem Wurfspieß, weshalb man auch von „Spearphishing“ spricht.

Die Schreiben geben vor, vom oberen Management, aus der Vereinsführung oder aus dem Präsidentenbüro zu stammen. Sie sollen betroffene Mitarbeiter aus Buchhaltungen respektive

Kassenwarte überrumpeln, kurzum: Personen, die Überweisungen im Auftrag ihrer Institution ausführen dürfen.

Sofort, dringend überweisen!

Auch das inhaltliche Schema, mit dem die Täter Frieda K. hinters Licht führen wollten, ist typisch. Der Absender und die Interna zur Betriebserweiterung sollten ihr ein Gefühl von Authentizität geben, obwohl die Mail ungewöhnlich war und die Handlungsanweisung gegen interne Regeln und Konventionen verstieß.

Der dringliche Charakter des Schreibens und die in Aussicht gestellte Gehaltserhöhung hatten das Ziel, Frieda K. zu schnellem Handeln zu verleiten und auf Rückfragen verzichten. Alternativ hätte die Mail auch Drohungen oder Schmeicheleien enthalten können. Eine Antwort auf die Mail wäre bei den Tätern gelandet, die mit weiteren Interna oder emotionalem Druck zurückgeschrieben hätten.

Hätte Frieda K. die gefälschten Anweisungen befolgt und den Betrag ohne die sonst übliche Prüfung überwiesen, wäre er auf einem von den Betrügern kontrollierten Konto gelandet. Im Fall von Frieda K. befand sich das Konto in Übersee, außerhalb der Reichweite deutscher Ermittler. Doch auch bei einem Konto in Deutschland hätten die Täter die Beute rasch weiter ins Ausland überwiesen und so den Verbleib verschleiert.

Wohlinformierte Täter

Die Täter operieren in gut organisierten Banden und spähen Firmen professionell gezielt aus. Dabei nutzen sie zunächst alles, was sie frei zugänglich finden. Bereits die Websites vieler Firmen bieten einen mehr oder minder großen Fundus: Inhaber und einzelne Mitglieder der Geschäftsleitung sind immer namentlich genannt. Man findet sie im juristisch obligatorischen Impressum, oft aber auch in Unternehmensporträts. Ebenso präsentieren viele Firmen ihre

Geschäftsfelder samt Geschäftspartnern auf der Homepage. Für bestimmte Geschäftsbereiche verantwortliche Manager oder Ansprechpartner für Kunden erhalten häufig eine eigene Bühne.

Oftmals ergattern die Täter jedoch auch Informationen, die für die Außendarstellung des Unternehmens nicht erforderlich sind. Dazu gehören beispielsweise Organigramme oder andere Hinweise auf Namen von Mitarbeitern, die Zahlungen ausführen – eine wahre Goldgrube für Kriminelle, denn selbst wenn die Mailadresse fehlt, können sie diese aus dem Schema erschließen. Wenn man den Vertriebsleiter unter max.mustermann@angriffsziel.de erreicht und weiß, dass die Buchhalterin Frieda K. heißt, ist frieda.k@angriffsziel.de naheliegend.

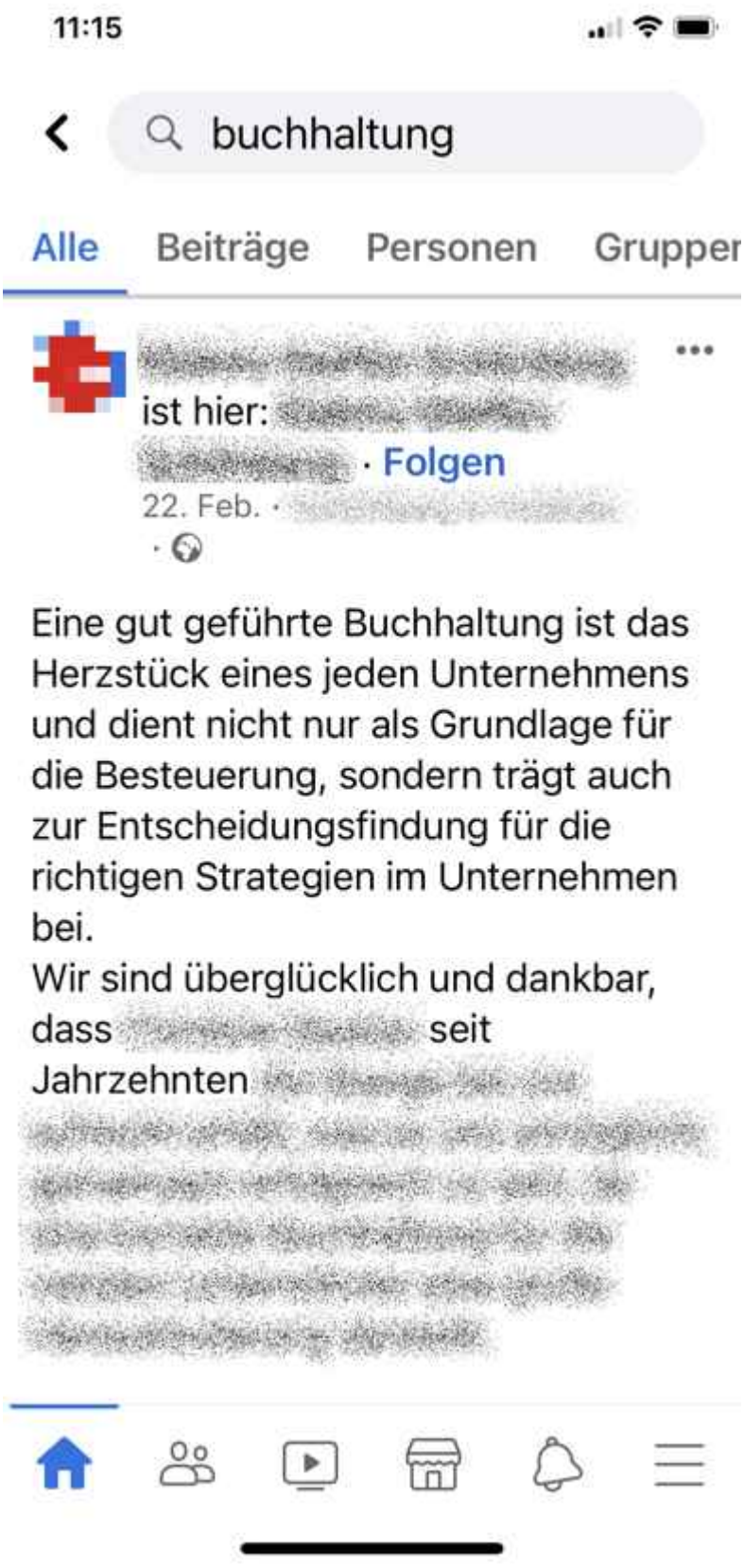
Je nach Organisationsform der Firma gewinnen Täter außerdem Wissen aus den Einträgen im Handelsregister sowie den Unternehmensabschlüssen im Bundesanzeiger. Diese verraten zum Beispiel Geschäftsmodelle oder Bilanzvolumina, aus denen die Täter realistische Summen für einzelne Aufträge ableiten.

Eine weitere Fundgrube stellen die Social-Media-Auftritte dar. Manche Unternehmen plaudern dort erstaunlich zwanglos über ihre Prozesse und ihre Beschäftigten – oder die Mitarbeiter selbst berichten auf ihrem privaten Twitter- oder Instagram-Account über ihre Firma, ihre Kollegen und deren Tätigkeiten.

Noch ergiebiger sind für die Täter allerdings Zugänge zu echten Interna. Bei vielen (oftmals unerkannten) Angriffen auf die IT-Systeme von Unternehmen schnorcheln die Hacker als Hauptziel oder Beifang alle Informationen ab, die sie bekommen können. Diese verwenden sie dann entweder selbst oder verkaufen sie an spezialisierte Banden.

Zur Beute gehören Mails, Geschäftsprozesse und Planungsunterlagen samt Namen und Zuständigkeiten. Vieles davon gibt zusätzlich Aufschluss über externe Geschäfts- und Ansprechpartner. Diese Unternehmen und Personen geraten nun

ebenfalls ins Fadenkreuz. Denkbar ist außerdem ein Mitarbeiter, der bewusst oder unbewusst Interna weitergibt. Je detaillierter die Täter eine Organisation kennen, umso gezielter können sie einzelne Mitarbeiter attackieren.



Aus der lobenden Erwähnung der Buchhaltung können auch Betrüger Schlüsse ziehen.

Gegenmaßnahmen im Unternehmen

Vor diesem Hintergrund müssen kleine wie große Unternehmen das Angriffspotenzial erfassen und minimieren. Dabei kommt es nicht nur auf eine gute IT-Sicherheitsstrategie an, um unbemerkte Einbrüche in das Unternehmensnetzwerk zu verhindern, sondern auch auf eine überlegte Kommunikation.

Nach außen hin müssen Unternehmen sorgfältig abwägen, wie umfangreich sie sich darstellen. Ein Beispiel: Oft gilt es als Zeichen der Wertschätzung, möglichst das gesamte Team mit Namen, Funktion und womöglich Kontaktdaten zu präsentieren. Doch das birgt zugleich das Risiko, dass Kriminelle dieses Wissen ausnutzen.

Intern sollten Unternehmen ihre Mitarbeiter über denkbare Betrugsmaschen aufklären und für Angriffe sensibilisieren – insbesondere für den Fall, dass sie ungewöhnliche, vermeintlich interne Anweisungen erhalten. Dabei helfen robuste Prozesse ohne Ausnahmen (auch keine informellen), um Zahlungen an Kunden oder Lieferanten auf Authentizität zu prüfen und Überweisungen freizugeben. Für regelwidrige Aufforderungen brauchen Mitarbeiter ein verlässliches Meldeverfahren, kompetente Ansprechpartner und die Gewissheit, dass ihnen bei Fehlalarmen keine Konsequenzen drohen.

Dabei müssen Unternehmen sämtliche Mitarbeiter auf ein gesundes Misstrauen verpflichten und ihnen verdeutlichen, dass Angreifer bereits aus der vermeintlich harmlosen Außenkommunikation viele interne Informationen gewinnen. Ebenso sollte es zur Unternehmenskultur gehören, die eigenen Security-Maßnahmen nicht als unfehlbar zu betrachten, sprich: Jedes Unternehmen muss davon ausgehen, dass die Täter bei Social-Engineering-Angriffen Informationen besitzen, die sie durch Einbrüche ins eigene Netz oder die Systeme von

Geschäftspartnern erlangt haben. Anders ausgedrückt: Eine Mail oder ein Anruf sind noch lange nicht authentisch, wenn sie vermeintliche Insider-Informationen enthalten.

Tipps für Mitarbeiter

Die Beschäftigten selbst müssen sich ausnahmslos an die Verfahrensvorgaben halten, insbesondere für Buchhaltung und Zahlungen, und dürfen auch unter Druck nicht von den Regeln und Prüfmechanismen abweichen. Gerade solche Mails wie die an Frieda K. oder auch Anrufe bedürfen einer sorgfältigen Prüfung – nach dem alten Grundsatz „Vertrauen ist gut, Kontrolle ist besser“. Selbst wenn der angezeigte Name in einer Mail stimmt, kann die eigentliche Mailadresse abweichen. Bei Anrufen kann man die Anrufernummer technisch leicht fälschen, bald wohl auch die Stimme. Bei ungewöhnlichen Nachrichten zieht man daher Kollegen und Vorgesetzte hinzu, am besten auch die IT-Sicherheitsabteilung.

Sämtliche Mitarbeiter müssen Mails grundsätzlich mit Vorsicht behandeln. Links können auf präparierte Websites führen, Anhänge Schadcode enthalten. Beides öffnet Angreifern womöglich die Tür in die Unternehmenssysteme und liefert ihnen die Munition, die sie für Spearphishing gegen das eigene Unternehmen oder Geschäftspartner brauchen; von anderen Bedrohungen wie Ransomware oder dem Diebstahl von Geschäftsgeheimnissen ganz zu schweigen.

Genau wie die Unternehmen selbst sollten Mitarbeiter keine Interna mit Dritten teilen. Das betrifft besonders den digitalen Raum: Informationen über die Tätigkeit von Kollegen oder Strukturen im Unternehmen gehören nicht auf Instagram & Co. Aber auch das persönliche Gespräch auf Messen oder in Meetings kann kritisch werden, wenn es sich um Details zu Hierarchien, Prozessen und Sicherheitsmaßnahmen dreht.

Egal ob der Betrugsversuch glückt oder nicht: Unternehmen sollten bereits beim Verdacht Beweise wie Mails sichern, den

Fall dokumentieren und Anzeige bei der Polizei erstatten. Die Wahrscheinlichkeit, dass diese die Täter ermittelt, mag gering erscheinen. Ohne Anzeige ist sie jedoch null. Außerdem lohnt es sich, den Vorfall intern zu kommunizieren und Mitarbeiter wie Geschäftspartner zu warnen – vielleicht nehmen die Betrüger schon den nächsten Kollegen ins Visier. Wenn Dritte in die Systeme eingedrungen sind und sensible Informationen entwendet haben, sind Unternehmen in vielen Fällen außerdem nach DSGVO verpflichtet, mögliche Geschädigte wie zum Beispiel Geschäftspartner zu informieren. Ohnehin ist das ein Gebot der IT-Sicherheit, damit sich auch Dritte gegen mögliche Angriffe wappnen können.

Variante: Rechnungsbetrug

Verwandt mit dem CEO-Betrug ist der Invoice- oder Rechnungsbetrug. Auch bei dieser Masche haben sich die Täter Insiderwissen über Geschäftsbeziehungen eines Unternehmens besorgt. Sie kennen die zuständigen Mitarbeiter aus der Buchhaltung oder wissen, dass der Inhaber selbst die Rechnungen von seinen Lieferanten und Dienstleistern begleicht.

In einem c’t bekannten Fall erhielt der Buchhalter eines mittelständischen Unternehmens eine Mail. Der Absender schien der Vertriebsleiter eines langjährigen Lieferanten aus Japan zu sein. Die Mailadresse der Firma wich zwar von der bekannten ab, las sich aber plausibel.

Freundlich fragte der „Vertriebsleiter“ im üblichen nicht ganz korrekten Englisch, ob es noch offene Rechnungen gebe und wenn ja, welche. Es sei wichtig und dringend: Man habe ein Problem mit dem bisherigen Konto und ein neues eröffnet. Nun wolle man sichergehen, dass kein Geld an die alte Verbindung fließe.

Der Buchhalter schöpfte keinen Verdacht und übermittelte ihm die Rechnungsnummern von zwei Lieferungen (eine davon bereits überwiesen) samt der hohen vierstelligen Rechnungsbeträge. Auf

zusätzliche Rückfrage nannte der Buchhalter auch das Überweisungsdatum der einen und die Zahlungsfrist der anderen Rechnung.

Artig bedankte sich der vorgebliche japanische Vertriebsleiter und nannte die neue Bankverbindung, „ein Konto unserer Zweigstelle in Australien“. Die noch offene sowie alle zukünftigen Zahlungen solle man dorthin überweisen. Der Buchhalter tat, wie ihm geheißen, und änderte die Bankverbindung in den eigenen Systemen. Offenbar schien alles geklappt zu haben, denn nach der Überweisung zum vereinbarten Termin meldete sich der „Vertriebsleiter“ erneut und bedankte sich für den Zahlungseingang.

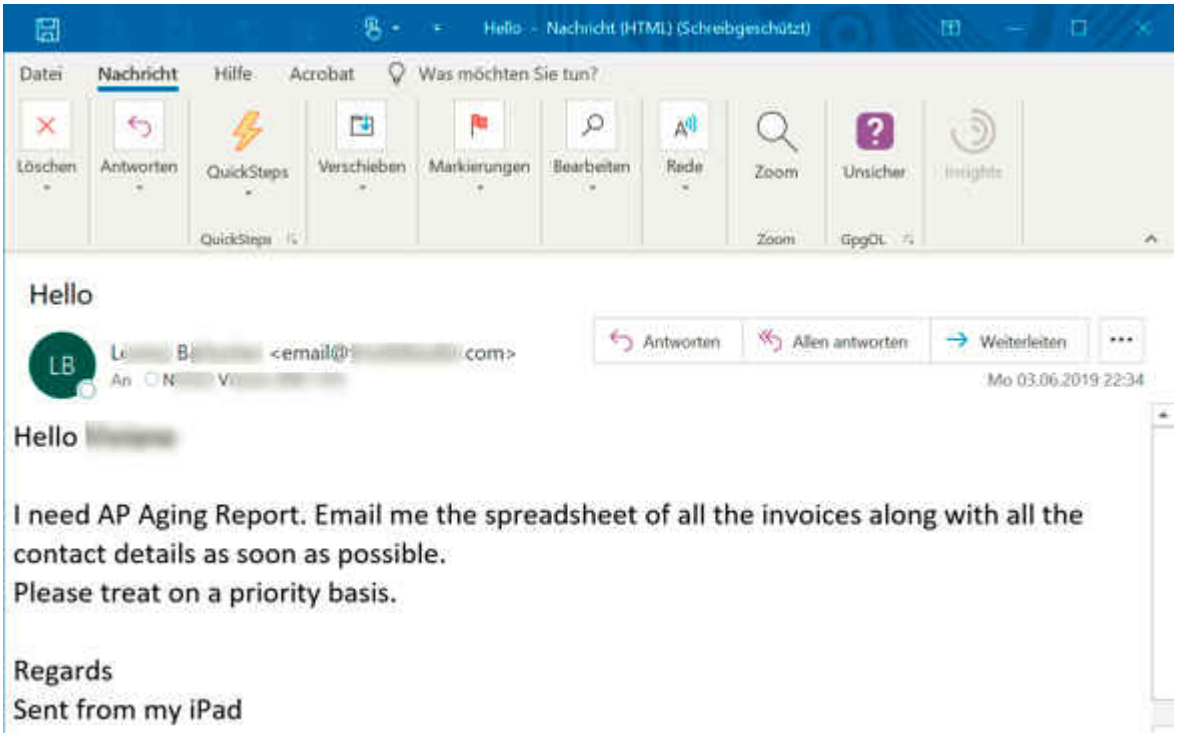
Der Buchhalter war beruhigt, bis ihn zwei Tage später die tatsächlichen Kollegen des japanischen Unternehmens anschrieben und höflich an die noch ausstehende Zahlung erinnerten. Die habe er doch auf das neue Konto überwiesen, ließ er wissen. Nachdem ihm die Japaner jedoch versichert hatten, dass es kein neues Konto gebe und die erste Zahlung regulär eingegangen sei, dämmerte ihm, dass er einem Schwindel aufgesessen war.

Parallelen und Prävention

Die Muster gleichen denen des CEO-Betruges: Mit Insiderwissen und bekannten Namen zielen die Täter auf Firmenangehörige mit Zahlungsbefugnis oder Selbstständige. Sie gaukeln aber keinen neuen Geschäftspartner vor, sondern eine Kontoänderung bei einem bestehenden Kontakt. Die Interna besorgen sich die Täter genau wie beim CEO-Betrug. Der Angriff erfolgt meistens per Mail, kann aber auch telefonisch oder postalisch ablaufen.

Die Polizei warnt außerdem, dass Täter alternativ zu angeblichen Kontoänderungen auch immer häufiger versuchen, den Opfern komplett erfundene Rechnungen unterzuschieben. Bei der Prävention gibt es in beiden Fällen von klar definierten Prozessen bis zur internen und externen Kommunikation kaum

Unterschiede zum CEO-Betrug – bis auf einen: Um einen Rechnungsbetrug bei einer Zahlung auszuschließen, benötigen Unternehmen in diesem Fall fest vorgegebene Wege, um Kontoänderungen bei regelmäßigen Lieferanten und anderen Geschäftspartnern zu verifizieren. Insbesondere sollte man nicht direkt auf eine verdächtige Mail reagieren, sondern die Kontaktdaten aus vorangegangener Korrespondenz nutzen und am besten anrufen – und dafür gleichbleibende Ansprechpartner vereinbaren.



Die Täter bahnen einen Rechnungsbetrug an und fragen gezielt nach weiteren offenen Posten – oft deutlich eleganter als in diesem Fall.

Überschreitet eine Rechnung einen Schwellwert, helfen zusätzliche formelle Wege, um die Kontoverbindung zu bestätigen. Denkbar ist zum Beispiel, sich mit dem Geschäftspartner in einer Videokonferenz zu treffen. Die Zahlung bestätigt man anschließend per Mail, einschließlich der Namen der Banken und den letzten vier Ziffern der Kontonummer. Wie beim CEO-Betrug gilt auch hier: Bereits den Versuch sollte ein Unternehmen sorgfältig dokumentieren und bei der Polizei anzeigen. (*mon@ct.de*)

Lastschrift-Betrug gegen kleine Händler

Derzeit versuchen Kriminelle gezielt, kleine, meist inhabergeführte Onlineshops mit Lastschriftzahlungen übers Ohr zu hauen. Zunächst bestellen sie im Namen beliebiger Personen samt passender Mailadressen einen größeren Posten für mehrere tausend Euro. In einem c’t bekannten, zur Anonymisierung leicht abgewandelten Beispiel orderten sie bei einem Sportartikelhändler mehrere hundert Bälle.

Als Zahlungsart wählen die Täter SEPA-Lastschrift. Das Konto des „Kunden“ befindet sich häufig im EU-Ausland; im vorliegenden Beispiel wies die IBAN auf die italienische Dépendance der französischen Business-Digitalbank Olinda („Qonto“). Da es sich um betrügerisch eröffnete Konten handeln dürfte, sind aber auch deutsche Konten denkbar, beispielsweise bei N26 [1].

Wenig später schicken die Täter eine Mail. Als vorgeblicher „Kunde“ schreiben sie, dass ihnen ein Zahlendreher unterlaufen sei. Daher würden sie um eine Bestellungs- und Rechnungskorrektur bitten, in unserem Beispiel von 150 auf 15 Stück – eine typische Größe für eine Trainingsgruppe.

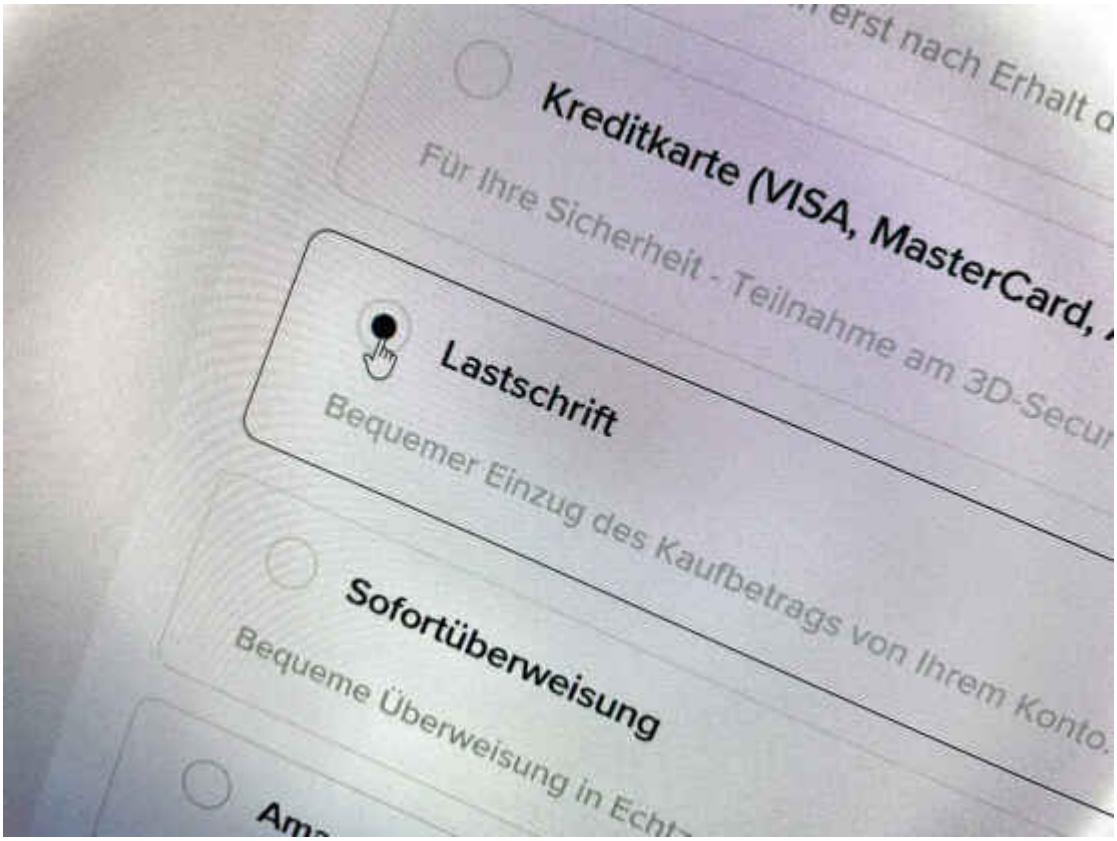
Im Kalkül der Täter erstattet der Händler die Differenz nun zurück, entweder per Banküberweisung oder über seinen Zahlungsabwickler (Payment Service Provider, PSP). Erfolg haben sie aber auch, wenn der Händler misstrauisch wird, den Auftrag storniert und den kompletten Betrag zurücküberweist. Sobald das Geld nämlich auf dem von den Tätern kontrollierten Konto landet, buchen sie die Lastschrift ebenfalls zurück (Rücklastschrift). Der Händler kann dies ebenso wenig umkehren wie die Überweisung und hat nun einen Schaden in Höhe des Überweisungsbetrages.

Bei der Masche nutzen die Täter die Regeln für das Lastschriftverfahren aus: Kunden können eine Lastschrift ohne Angabe von Gründen acht Wochen lang bei ihrer Bank widerrufen;

die Bank holt das Geld ohne weitere Nachfrage zurück. Der Händler muss eine berechtigte Forderung dann auf dem Rechtsweg geltend machen. Weder sein PSP noch seine Bank können den Inhaber des betrügerisch genutzten Kontos ermitteln; das dürfen nur Strafverfolgungsbehörden auf eine Anzeige hin. Da die Täter das Konto in diesem Fall jedoch unter falscher Flagge und dazu im EU-Ausland führen, kann man sie und das Geld kaum noch ausfindig machen.

Den Tätern hilft bei der Masche, dass viele Händler ihren Kunden mit einem Vertrauensvorschuss begegnen und ihnen bei Fehlern kulant entgegenkommen. Zudem sind in kleinen Onlineshops keine Zahlungsverkehrsexperten tätig. Generell stehen Händler beim Lastschriftverfahren nämlich vor einem Dilemma: Es ist bei deutschen Kunden als sichere Bezahlmethode sehr beliebt und für den Händler sehr preisgünstig. Durch die Möglichkeit der Rücklastschrift besteht aber ein erhöhtes Betrugsrisiko.

Experten raten daher, dass ein Händler Lastschriften mit hohem Volumen nicht an unbekannte Kunden zurücküberweisen sollte – auch nicht teilweise. Stattdessen teilt er dem Kunden per Mail mit, dass der Shop die Bestellung vollständig storniert habe. Der Kunde möge bitte selbst eine Rücklastschrift bei seiner Bank veranlassen. Um Schäden von vornherein zu begrenzen, kann der Händler mit seinem PSP außerdem eine Obergrenze für Lastschriften vereinbaren. Wenn der Zahlungsbetrag darüber liegt, bekommen Kunden an der Onlinekasse nur noch andere Zahlungsarten angeboten.



Onlinehändler schätzen an der SEPA-Lastschrift den günstigen Preis und fürchten das erhöhte Betrugsrisiko.
Im Regelfall kann ein Händler nämlich nicht hoffen, den Schaden aus einer betrügerischen Lastschrift vom PSP ersetzt zu bekommen. Normalerweise schließt er dies in seinen AGB aus, weshalb man auch von „nicht abgesicherten“ Lastschriften spricht. Einige PSP, etwa Ratepay und Klarna, bieten zwar sogenannte „abgesicherte“ Lastschriften an und übernehmen das Ausfallrisiko. Das lassen sie sich vom Händler aber mit höheren Entgelten bezahlen.

Auch die Wahl des PSPs spielt eine Rolle. Einige machen es den Tätern leichter als andere. Das beginnt bei der Aufklärung über Risiken bestimmter Zahlungsmethoden wie der SEPA-Lastschrift sowie Empfehlungen zum Ablauf von Rückerstattungen. Leitfäden für Händler sollten verständlich sein, der Support die eigene Sprache sprechen und mit den landestypischen Zahlungsmethoden vertraut sein – SEPA-Lastschrift ist zwar ein europäisches Verfahren, aber vor allem in Deutschland gebräuchlich. Auch eine automatische Betrugserkennung sowie konkrete Hilfestellungen in konkreten

Rückerstattungsfällen sind hilfreich.

Ein c’t bekannter Fall betraf den irisch-amerikanischen Dienst Stripe: Obwohl der Händler einen Betrugsversuch erkannte, kam es zu einem Missverständnis, als er den Betrugserkennungs-Ratgeber konsultierte. Er überwies daraufhin die Lastschrift zurück und verlor sein Geld; der ohnehin nur englischsprachige Chat-Support von Stripe lehnte eine Erstattung unter Verweis auf die Nutzungsbedingungen ab.

1. Literatur
2. Markus Montz, Vom Bankentester zum Geldwäscher, Wie Cyberkriminelle arglose Jobsucher rekrutieren, c’t 3/2023, S. 126