Cyber-Crime

Die dreisten Tricks im Maschinenhandel

Geschickte Betrüger nutzen das Internet, um Händlern sensible Daten und Geld zu stehlen. Welche Methoden wenden die Diebe an und wie wehrt man sich dagegen?

© *fotoia.com/zephyr_p*

Die Täter sind sehr geschickt und kreativ. Bei allen Transaktionen im Internet sollte man aufmerksam und wachsam sein.

Ein Landmaschinenhändler soll für einen Kunden eine bestimmte Gebrauchtmaschine ausfindig machen. Er stöbert sie bei einem ausländischen Berufskollegen auf und schickt nach einem einleitenden Austausch einen Mitarbeiter zur Begutachtung der Maschine. Alles läuft seriös ab und ein gegenseitiges Vertrauen ist vorhanden. Den weiteren Austausch führen beide Händler per E-Mail, um Missverständnisse aufgrund der Sprachbarriere auszuschalten. Denn die Konversation läuft auf Englisch ab. Schon bald werden sich beide Parteien einig und die Überweisung des Kaufbetrages erfolgt auf das in der Rechnung genannte Konto. Doch nach drei Wochen wartet der deutsche Händler immer noch auf die Maschine, während der ausländische Kollege noch kein Geld bekommen hat.

Was beide nun mit Entsetzen feststellen mussten: Sie wurden Opfer eines dreisten Trickbetrügers. Der Gauner fing die Mails der beiden Händler während der gesamten Kommunikation ab und fingierte die jeweilige Antwort-Mail, bevor diese beim vorgesehenen Empfänger eingingen. Schlussendlich übermittelte der Betrüger auf diese Weise seine Bankdaten anstelle der des ausländischen Händlers und kam so an das Geld.

„Dieser Fall, der sich 2017 wirklich zutrug, ist leider keine Ausnahme“, erklärt Pierre Büttner von der Plattform „Farmpartner-Tec“. Nicht nur mit dem hier geschilderten „Spoofing“ greifen Betrüger gezielt auch den Landmaschinenhandel an, um Geld zu ergaunern.

Wie Büttner aus stetigen Recherchen, Dialogen mit betroffenen Händlern und auch durch einen engen Austausch mit der Kriminalpolizei weiß, sind Internetbetrüger sehr erfindungsreich.

Folgende Tricks sind beliebt:

- Kleine Programme in Spam-Mails installieren sich auf dem Rechner und übermitteln sensible Daten.
- Gefälschte Internetseiten fischen Daten ab, die die Diebe für ihre Zwecke nutzen.
- Mit geschickter Manipulation fordern die Betrüger Händler auf, Geldbeträge zu überweisen.

Tückische Anhänge in Spam-Mails

Mailanhänge können Viren oder Trojaner enthalten, die das Betriebssystem des Händlers sabotieren. „Öffnet der Empfänger die Anhänge, gelangen diese kleinen Programme auf seinen Rechner und können ihren Dienst verrichten“, warnt Büttner. Da viele Kunden um das Problem wissen, lassen die Täter die Mails möglichst harmlos und natürlich erscheinen. Das können z.B. Mahnungen, Information über eine Paketzustellung, eine Rechnung des Telefondienstleisters oder des Stromversorgers sein. Meist sind die Anhänge in sogenannten komprimierten Zip-Dateien oder PDFs enthalten.

Tückisch sind auch vermeintliche Bewerbungsschreiben, vor allem, wenn der Händler Stellenausschreibungen auf seiner Internetseite hat. Die Täter senden dann mit Verweis auf die Ausschreibung eine Bewerbung und verweisen auf Unterlagen im Anhang. Meist ist das auch eine ZIP-Datei mit enthaltenen „.doc.js“-Anhängen, durch die Viren installiert werden. „Besonders beliebt ist aktuell die Ransomware WannaCry“, beschreibt Büttner. Sie verschlüsselt Dateien auf dem Rechner. Zum Entschlüsseln soll der Nutzer meist mehrere hundert Euro für einen Freischaltcode überweisen.

Ein Trojaner dagegen fordert den Nutzer nicht gleich zum Handeln auf, sondern arbeitet unauffällig im Hintergrund. Er hat das Ziel, Daten oder Eingaben mithilfe von Zwischenstationen abzufangen, zu manipulieren und für unseriöse Zwecke zu nutzen. Beispiel: Man öffnet als Nutzer die Internetseite seiner Bank. Die Homepage erscheint dabei wie immer. Allerdings kann der Trojaner bestimmte Bestandteile verändert haben, was äußerlich nicht zu erkennen ist. Im Hintergrund arbeiten dabei Softwaretools oder Funktionen eines Dritten. Trägt man wie gewohnt Daten ein wie das Passwort oder eine Transaktionsnummer (TAN) bei einer Online-Überweisung, können die Daten manipuliert werden. „Die Betrüger verändern z.B. den Überweisungsbetrag und fügen ihre eigene Kontodaten ein“, schildert Büttner ein mögliches Vorgehen. Der Geschädigte merkt den Betrug oft erst, wenn er seinen Bankauszug sieht.

Gefälschte Internetseiten

Neben Trojaner oder Viren nutzen einige Betrüger auch das so genannte „Pharming“: Dieses bewirkt, dass die sogenannte IP-Adresse einer Internetdomain verändert wird. Gibt der Händler dann z.B. den Domainnamen seiner Bank „www.meineBank.de“ ein, wird nicht das gewollte Ziel angesteuert, sondern ein vollkommen anderes. „Wenn die nachgeahmte Bankseite gut gemacht ist, merkt man als Benutzer von alledem nichts und trägt wie gewohnt seine Daten ein“, sagt Büttner. Auch damit können die Täter sensible Daten wie Passwörter usw. abgreifen, um im Namen des Opfers Bankgeschäfte durchzuführen.

Ähnlich funktioniert das Phishing, bei der die Täter den Benutzer dazu bringen, eine Website mit einem passwortgeschützten Premiumbereich aufzurufen. Dazu schicken sie unter einem Vorwand einen Link in der Mail mit dem Aufruf, die Seite zu besuchen. Allerdings haben sie bei der Internetadresse meist einen kleinen Fehler eingebaut, z.B. einen Buchstaben vertauscht. Unbemerkt wird der Nutzer zunächst auf die gefälschte Seite geleitet, gibt dort wie gewohnt sein Passwort ein und gelangt nachfolgend auf die Originalseite. Den Zwischenschritt haben die Täter aber genutzt, um Passwort und Benutzername „abzufischen“. „Damit können sie die Identität des Landtechnikhändlers nutzen, um beispielsweise Angebote von gebrauchten Maschinen zu manipulieren und potenzielle Käufer dieser Maschinen dazu zu bringen, in Kontakt mit dem Händler zu treten“, erklärt der Internetfachmann.

Zu diesem Zweck werden häufig die Preise der Angebote drastisch reduziert und da die Maschinen wirklich existieren, wirken die veränderten Angebote besonders realistisch. Damit gaukeln die Täter Käufern ein Schnäppchen vor. Der Käufer glaubt das zumindest. Aber weil E-Mail und Telefonnummer der im Angebot enthaltenen Händlerangaben zuvor verändert wurden, tritt er gar nicht in Kontakt mit dem seriösen Händler, sondern – ähnlich wie beim eingangs geschilderte „Spoofing“-Fall – mit einem Betrüger. Bei der Kontaktaufnahme wird den Interessenten eine Geschichte aufgetischt, z.B. dass die Maschine noch im Ausland steht. Soll sie dem Verkäufer vorgeführt werden, müsste sie erst nach Deutschland gebracht werden. Dafür müsste der Käufer lediglich im Vorfeld die Transportkosten überweisen. Hat der Käufer das getan, ist er sein Geld los. Ähnlich funktioniert die Masche, dass die Täter die Internetpräsenz eines Händlers identisch nachstellen. So einen Fall hat es erst Ende 2016 bei einem Landmaschinenhändler gegeben. Hier haben die Täter lediglich bei der URL des Händlers das Wort „Landtechnik“ durch „GmbH“ ausgetauscht. „Die Seite glich dem Original wie ein Ei dem anderen und der Unterschied war so für einen Besucher nicht zu erkennen“, schildert Büttner. Auch hier waren dann die Preise der Maschinen herabgesetzt und es gab die gleichen Folgen wie beim „Phishing“: Der potenzielle Käufer überweist Geld für den Maschinentransport aus dem Ausland. Am Ende gibt es zwei Geschädigte: der um sein Geld geprellte „Käufer“ und der Händler, dem ein Imageschaden entsteht und der viel Zeit in die Aufklärung investieren muss.

Vermeintlicher Supportdienst

Bei der als „Vishing“ bezeichneten Betrugsmasche rufen Mitarbeiter eines Callcenters beim Händler an und berichten, dass bei seinem Betriebssystem Viren oder andere Fehler entdeckt wurden, der Dienstleister diese aber beheben könne. Gerne geben sich die Anrufer hierbei als Mitarbeiter von Microsoft aus, dem Lieferanten des Betriebssystems „Windows“.

Er bräuchte lediglich Zugriff auf den Rechner über ein Fernwartungsprogramm wie Teamviewer. Der gutgläubige Kunde gewährt ihm Zugang und bemerkt nicht, dass der Täter daraufhin den Virenscanner deaktiviert und Virensoftware installiert. Auch damit lassen sich sensible Daten ausspähen. Am Ende des Gesprächs soll der Kunde dann einen kleinen Obolus zahlen wie z.B. 30 Euro. Überweist er diesen Betrag, kann der Täter mit der im Vorfeld auf dem System installierten Schadsoftware die Banktransaktion überwachen und wie bei einem Trojaner den Geldbetrag deutlich erhöhen.

Auch eine erfolgreiche Masche ist der CEO-Fraud, bei dem der Chef per Mail vermeintlich seine Buchhaltung auffordert, einen bestimmten Geldbetrag zu überweisen.

E-Mail vom Chef

Das Tückische dabei: Der Absender gibt sich als Geschäftsführer (CEO) aus und schreibt exakt mit dessen Adresse. „Absendeadressen kann man mit jedem handelsüblichen Mailserver ohne weiteres fälschen, dazu muss man nicht mal IT-Experte sein“, warnt Büttner.

In diesem Fall geht beim Buchhalter eine Mail mit dem Text: „Leider bin ich heute nicht im Büro, aber muss sofort eine Überweisung für eine dringende Ersatzteillieferung (oder Maschinenlieferung) vornehmen.“ Um den Buchhalter in Sicherheit zu wiegen, bittet der vermeintliche Chef erst um schriftliche Bestätigung, bevor dieser die Bankdaten in einer weiteren Mail schickt. Die Bestätigung geht an eine andere Empfängeradresse, die jeder als Antwortadresse in einer Mail hinterlegen kann. Der Betrüger erhält diese, um erneut an den Mitarbeiter zu schreiben. Wie Büttner erklärt, werden dabei durchaus Beträge von 70.000 bis 100.000 Euro gefordert. Viele loyale Buchhalter reagieren königstreu und überweisen den Betrag, ohne an der Echtheit der Mail zu zweifeln. Die Überweisung erfolgt zumeist auf ein Western Union Account, eine Rückbuchung ist kaum möglich.

Manipulierter Bankautomat

Vor allem Außendienstmitarbeiter können Opfer des so genannten Skimmings werden. Auch hierbei werden sensible Daten ausgespäht. Das passiert an Bankautomaten oder Stationen für Kreditkartenbezahlung. „Gerade häufig frequentierte Terminals an Raststätten werden dafür genutzt“, sagt Büttner. Mit einem kaum zu erkennenden Vorbauscanner können die Täter den Magnetstreifen der Kreditkarte auslesen. Außerdem bringen sie auf der Tastatur eine weitere Tastatur auf oder installieren eine kleine Kamera im Schirm über der Tastatur. Mit beiden können sie die PIN des Opfers auskundschaften. Anschließend übertragen sie die Magnetstreifendaten auf eine Blankokarte und heben Geld vom Konto ab. „Davon betroffen sind vor allem Privatkunden, aber auch Außendienstmitarbeiter, die z.B. eine Maschine oder ein Fahrzeug tanken und mit der Firmenkreditkarte zahlen“, weiß Büttner.

Wie Sie reagieren können

Die geschilderten Fälle sind lediglich ein grober Überblick über mögliche Betrugsmaschen. „Die Täter werden immer geschickter und sind extrem kreativ“, hat Büttner festgestellt.

Trotzdem sind Sie nicht schutzlos. So können Sie mit folgenden Maßnahmen zumindest einen Teil der Betrügereien abwehren:

- Bei allen Transaktionen im Internet sollten Sie sehr aufmerksam und immer wachsam sein: Ist der vermeintliche Geschäftspartner auch seriös?
- Seien Sie vorsichtig bei Zahlungsaufforderungen an ausländische Konten wie z.B. „Western Union“ oder bei ausländisch sprechenden „Callcentern“.
- Das gleiche betrifft auch die Mitarbeiter. Sie sollten lieber zweimal telefonisch nachfragen, bevor sie eine dubiose Überweisung tätigen.
- Selbst bei Telefonkommunikation sollten Sie vorsichtig mit der Weitergabe von Daten sein.
- Sie sollten auf dem Rechner keine Passwörter speichern, auch nicht im Browser, denn diese lassen sich auslesen.
- Klicken Sie keine Links in E-Mails an. Geben Sie die Adresse lieber von Hand in das Browserfeld ein.
- Wenn Sie eine Zahlungsaufforderung von Ihrem Stromanbieter oder von der Bank erhalten, sollten Sie vorsichtig sein. Viele Institute weisen auf ihrer Internetseite darauf hin, dass sie diese Aufforderungen nie per Mail verschicken würden und ein Betrug vorliegen könnte.
- Öffnen Sie keine ZIP-Datei von einem unbekannten Absender. Vorsicht ist auch bei Kandidaten geboten, die sich auf eine Stellenausschreibung bewerben.
- Grundsätzlich sollten Sie noch nicht einmal eine Mail öffnen, wenn Absender und/oder Betreff nicht seriös erscheinen oder Sie Betreff, Text oder Absender nicht zuordnen können.
- Alle eingesetzten Geräte (Handys, Tablets, Rechner) sollten stets das aktuelle Betriebssystem und entsprechende Virensoftware besitzen.
- Beim eigenen W-LAN-Netzwerk sollten Sie nicht den voreingestellten, auf dem Gerät aufgedruckten Schlüssel nutzen, sondern ein eigenes Passwort verwenden. Sicher ist eine Kombination von Zahlen, Großbuchstaben und Sonderzeichen. Zudem verwenden Sie bitte immer die WPA2 Verschlüsslung.
- Am Übergang zwischen LAN und externem Netzwerk (z.B. einem Router) sollten Sie zumindest eine Softwarefirewall installiert haben.
- Auch an Ihrem Browser sollten Sie die entsprechenden Sicherheitseinstellungen vornehmen. Gute Browser weisen bereits auf unseriöse Webseiten und vermeintliche Schadsoftware hin.
- Sie sollten sich regelmäßig über Tricks und Maschen informieren, z.B. auf der Internetseite www.polizei-praevention.de