Leistungsabschreibung vs. degressive Abschreibung – mindern Sie Ihren Gewinn mit der richtigen Methode

Das Anlagevermögen bietet auch Ihrem Unternehmen ein breites Feld zur Steueroptimierung, besonders durch den Einsatz verschiedener Abschreibungsarten. Doch nicht jeder kennt die Bandbreite der Optionen, die über die klassische lineare Abschreibung hinausgehen. Könnten Sie sich beispielsweise zwischen der Leistungsabschreibung und der degressiven Abschreibung entscheiden? Nach diesem Artikel wird Ihnen die Entscheidung ganz sicher leichter fallen.

Schreiben Sie entsprechend der Leistung ab

Welche Abschreibungsarten haben Sie bisher in Ihrem Unternehmen in der Finanzbuchhaltung genutzt? Gucken Sie auch mal über den Tellerrand, denn es muss nicht immer die lineare AfA sein. Für bewegliche Wirtschaftsgüter des Anlagevermögens dürfen Sie die Abschreibung nämlich beispielsweise auch nach der Leistung des Wirtschaftsguts bemessen. Das kann -z. B. bei Produktionsmaschinen sinnvoll sein, die nach intensivem Einsatz an Leistungsfähigkeit verlieren.

BEISPIEL: Unternehmer (U) hat für sein Unternehmen eine neue Maschine zum Preis von 50.000 € gekauft. Die Maschine hat eine erwartete Lebensdauer von 10 Jahren und soll insgesamt 100.000 Einheiten produzieren. U plant, die Maschine über ihre Leistung abzuschreiben, was bedeutet, dass die Abschreibung auf der Anzahl der tatsächlich produzierten Einheiten basiert.

Im ersten Jahr nutzt U die Maschine intensiv und produziert 15.000 Einheiten. Um die Abschreibung für das Jahr zu berechnen, verwendet U die Formel:

Abschreibung = (Anschaffungskosten / Gesamtproduktionsmenge) x Jahresproduktion

Das ergibt:

Abschreibung = (50.000 € / 100.000 Stk.) x 15.000 Stk. = 7.500 €

Für das erste Jahr schreibt U also 7.500 € der Kosten der Maschine ab, basierend auf der Anzahl der produzierten Einheiten. Dies reflektiert den tatsächlichen Gebrauch der Maschine und verteilt die Kosten entsprechend ihrer Leistung über ihre Nutzungsdauer.

ACHTUNG

Die Leistungsabschreibung von Maschinen ist nur dann zulässig, wenn sie wirtschaftlich begründet ist, also die Abnutzung einer Maschine besser darstellt als beispielsweise die lineare Abschreibung. Sie können Nachfragen und Diskussionen in einer Betriebsprüfung bereits im Voraus verhindern, indem Sie Ihre Entscheidungen und Berechnungen gut dokumentieren.

Lohnt sich die degressive Abschreibung?

Im Rahmen des Wachstumschancengesetzes wird Ihnen in 2024 die Möglichkeit der degressiven Abschreibung eröffnet. Diese können Sie für Anlagegüter anwenden, die nach dem 01.04.2024 und vor dem 31.12.2024 angeschafft werden. Was gibt es hier zu beachten?

Bei der degressiven Abschreibung verringern Sie den Buchwert eines Wirtschaftsguts in fallenden Beträgen über die Nutzungsdauer. Der Abschreibungsbetrag wird dabei jedes Jahr auf den Restbuchwert des Vorjahres berechnet, was zu einer jährlich sinkenden Abschreibungsrate führt. Typischerweise verwenden Sie einen festen Prozentsatz, der höher ist als bei der linearen Abschreibung. Dieser Prozentsatz bleibt über die Jahre gleich, aber da er auf den jeweils verminderten Restbuchwert angewendet wird, sinkt der absolute Abschreibungsbetrag jedes Jahr.

Im Wachstumschancengesetz wurde bestimmt, dass die degressive Abschreibung das zweifache Ihrer linearen Abschreibung beträgt und 20 % nicht übersteigen darf. Betrachten wir das Beispiel mit Unternehmer (U), könnte er sich für die Abschreibung der angeschafften Maschine für die degressive Abschreibung entscheiden, wenn die Anschaffung zwischen dem 01.04.2024 und dem 31.12.2024 erfolgt ist. In diesem Fall würde U die Maschine im ersten Jahr mit

100 % / 10 Jahre = 10 % x 2 = 20 % abschreiben.

Ich habe den Abschreibungsbetrag für den Vergleich nicht anteilig berechnet.

Das ergibt:

Abschreibung = 50.000 € x 20 % = 10.000 €

Für das erste Jahr schreibt U also 10.000 € der Kosten der Maschine degressiv ab.

MEIN TIPP

Ein Übergang von der degressiven Abschreibung zur Leistungsabschreibung ist gesetzlich nicht verboten, sofern dieser nicht völlig willkürlich erfolgt.

Kennen Sie schon die Wirtschafts-Identifikationsnummer? Ab Herbst 2024 gilt sie für Unternehmen und Freiberufler

Aus Ihrem privaten Bereich oder von Ihren Arbeitnehmern kennen Sie die für Privatpersonen geltende Steuer-Identifikationsnummer. Im unternehmerischen Bereich war die Steuernummer oder die Umsatzsteuer-Identifikationsnummer bislang ein entsprechendes Pendant. Das soll sich zukünftig ändern. Ab Herbst 2024 wird die Wirtschafts-Identifikationsnummer eingeführt. Das müssen Sie dazu wissen.

Wer erhält die neue Nummer?

Die Wirtschafts-Identifikationsnummer (W-IdNr.) erhalten alle, die in Deutschland einer wirtschaftlichen Tätigkeit nachgehen. Diese Definition umfasst damit gleichermaßen

- natürliche Personen, die als Unternehmer oder Freiberufler tätig sind, und
- juristische Personen oder Personenvereinigungen.

Damit spielt es keine Rolle, welche Rechtsform Ihr Unternehmen hat. Sowohl Freiberufler als auch Einzelkaufleute sowie Kapital- und Personalgesellschaften werden mit der neuen Nummer ausgestattet. Gesetzliche Regelungen finden sich in § 139c AO. Dort ist auch festgehalten, welche Daten (neben der W-IdNr.) das Bundeszentralamt für Steuern (BZSt) zu Ihrem Unternehmen speichert.

ACHTUNG

Gehen Sie mehreren unternehmerischen Tätigkeiten nach? Dann werden Ihnen – getrennt nach den Tätigkeiten – auch mehrere W-IdNr. zugeteilt.

Nach Auskunft des Bundesfinanzministeriums soll die neue Nummer auf der einen Seite für eine eindeutige Trennung zwischen betrieblichem Bereich und privater Sphäre sorgen. Auf der anderen Seite wird sie auch die Abgrenzung einzelner Geschäftsfelder voneinander verbessern. Wichtig: Die W-IdNr. wird weder Ihre private Steuer-Identifikationsnummer noch Ihre bestehende Umsatzsteuer-Identifikationsnummer ersetzen. Insbesondere letztere bleibt weiterhin eine Pflichtangabe auf den von Ihnen ausgestellten Rechnungen.

Wozu dient die W-IdNr.?

Die neue Nummer soll zukünftig – ähnlich wie bei der Steuer-Identifikationsnummer im privaten Bereich – zur Identifizierung im Besteuerungsverfahren dienen. Heißt konkret: Sie werden diese Nummer bald zusätzlich zu Ihrer regulären Steuernummer auf Ihren Steuerbescheiden finden. Zudem wird die W-IdNr. im Unternehmensbasisdatenregister erfasst, das als Basis für die zentrale Erfassung von Unternehmensdaten dienen soll. Ziel ist es, die Kommunikation mit Behörden unter einer einheitlichen Nummer zu vereinfachen.

Wie wird die W-IdNr. vergeben?

Die wichtigste Information direkt vorab: Sie müssen sich um nichts kümmern, also insbesondere keinen Antrag stellen. Die neue Nummer wird nach Anforderung des für Ihr Unternehmen zuständigen Finanzamts vom BZSt vergeben. Von diesem erhalten Sie dann die Information über Ihre Wirtschafts-Identifikationsnummer.

Bereits heute weist das Bundesfinanzministerium darauf hin, dass nicht alle Nummern zur gleichen Zeit vergeben und versandt werden können. Das ist aus technischen und organisatorischen Beschränkungen schlichtweg nicht möglich. Der Versand erfolgt daher in Stufen. Eine bestimmte Reihenfolge ist hier nicht vorgegeben. Beschleunigen können Sie die Vergabe ebenso wenig.

ACHTUNG

Das BMF gibt einen wichtigen Hinweis: Verlangt ein Gesetz die Nennung der Identifikationsnummer von Ihnen, müssen Sie diese Angabe selbstverständlich erst ab dem Zeitpunkt der Bekanntgabe machen.

Wie setzt sich die Nummer zusammen?

Die Wirtschafts-Identifikationsnummer setzt sich wie folgt zusammen:

- Kürzel „DE“ für Deutschland
- 9 nachfolgende Ziffern
- ein Bindestrich
- ein 5-stelliges Unterscheidungsmerkmal

Beispielsweise könnte Ihre neue W-IdNr. das folgende Format haben: DE123456789-00001.

MEINE EMPFEHLUNG

Verfallen Sie nicht in Aktionismus. Ob die Vergabe der neuen Wirtschafts-Identifikationsnummer tatsächlich ab Herbst 2024 starten wird, ist noch nicht in Stein gemeißelt. Das Bundesfinanzministerium teilt dazu mit, dass es die Öffentlichkeit rechtzeitig über den Start des Vergabeverfahrens in Kenntnis setzen wird.

TOP-THEMA

IT-Sicherheit in Ihrer Buchhaltung: Mit diesen Tipps werden Sie nicht Opfer eines Phishing-Angriffs

Sie werden mir sicherlich zustimmen: Als Buchhaltungs-, Rechnungswesen-, Steuer- und Finanz-Profi muss man stets akkurat arbeiten, gleichzeitig aber auch eine hohe Arbeitslast stemmen. Eine enorme Herausforderung, die Sie und ich tagtäglich bewältigen müssen. Ich zeige Ihnen, warum Sie trotz dieses Pensums stets wachsam sein müssen. Die Bedrohung sind in diesem Fall nicht die Betriebsprüfer, sondern kriminelle Hacker.

Warum das Thema jeden treffen kann

Ich möchte mit 2 Beispielen aus meinem Arbeitsalltag starten, um Ihnen vor Augen zu führen, warum die Gefahr eines Phishing-Angriffs überaus real ist und auch Sie treffen kann.

BEISPIEL 1: Es erreichte mich vor ein paar Wochen die E-Mail eines Kunden. Als Absender war auf Anhieb die Einkaufsabteilung zu erkennen. Der Betreff lautete: Bitte aktualisieren Sie unsere Bestellnummer. Als Text war angegeben: Sehr geehrter Herr Haase, unsere Bestellung und damit auch die Bestellnummer, die zwingend auf Ihren Rechnungen anzugeben ist, haben sich geändert. Die Nummer und weitere Details finden Sie unter dem folgenden Link.

BEISPIEL 2: Meine Kollegen aus dem Bereich der Rechnungsprüfung haben per E-Mail die Rechnung eines großen amerikanischen Onlineversandhändlers erhalten. Das Logo und das Corporate-Design stimmten, der E-Mail-Text deutete auf bestelltes Büromaterial hin. Die Umsatzsteuer-Identifikationsnummer meines Unternehmens war angegeben, ebenso als Besteller der Name eines Kollegen. Die Rechnung sollte man sich über einen angegebenen Link herunterladen können.

Was haben diese beiden Beispiele gemeinsam? Es handelte sich um gezielte Betrugsversuche per Phishing-E-Mails.

Die aktuellen Zahlen des BSI sprechen eine deutliche Sprache: Hinter 66 % aller bei Ihnen eingehenden Spam-Mails steckt keine harmlose Werbung, sondern ein Cyberangriff. Klicken Sie auf einen der in den E-Mails angegebenen Links, drohen Ihnen in aller Regel die folgenden Attacken:

- Erpressung: Durch das Anklicken des Links laden Sie unbemerkt eine Schadsoftware (Ransomware) auf Ihren Rechner, die dafür sorgen kann, dass Sie durch Verschlüsselung keinen Zugriff mehr auf Ihre Daten und Programme erhalten. Erst nach Zahlung eines nicht geringen Geld- oder Bitcoinbetrags sollen Sie wieder in die Lage versetzt werden, Ihre Rechner zu nutzen. So zumindest das übliche Versprechen der Hacker. Ob dieses Versprechen tatsächlich im Nachgang eingehalten wird, ist natürlich keineswegs garantiert.
- Betrug: Sie werden per Link auf eine Internetseite geleitet, auf der Sie Daten (z. B. Unternehmensname, Adresse oder Bankverbindung) eingegeben sollen. So erlangen Kriminelle Informationen über Ihr Unternehmen oder Sie selbst als Person, die sie dann für weitere Angriffe nutzen können.

ACHTUNG

Selbst wenn Sie keine Daten preisgegeben – allein durch das Klicken auf den Link haben Sie den Kriminellen die Information geliefert, dass die verwendete E-Mail-Adresse korrekt ist. Im schlechtesten Fall nutzen Hacker diese Information, um weitere Angriffe vorzunehmen.

Die Zahlen des BSI zeigen zudem deutlich auf, dass Phishing-E-Mails in den meisten Fällen (rund 84 %) das Mittel der Wahl sind, wenn es um betrügerische Absichten der Kriminellen geht.

Buchhaltung als Hauptangriffsziel

Ich habe es bereits erwähnt: Ihr Arbeitsbereich bietet sich (leider) für gezielte Attacken nahezu an. Das liegt insbesondere an den beiden folgenden Aspekten:

- In Buchhaltung, Rechnungswesen, Steuer- oder Finanzabteilung laufen eine Vielzahl an Informationen zusammen. So haben z. B. nicht alle Mitarbeiter in Ihrem Unternehmen Kenntnis über Bankverbindungen. Zudem sitzen in den genannten Bereichen Personen, die über die Auszahlung von Geldern entscheiden dürfen. Und auf diese haben es Kriminelle in der Regel abgesehen.
- Aufgrund Ihrer Tätigkeit kommen Sie mit zahlreichen Geschäftspartnern in Kontakt. Dazu zählen insbesondere Kunden und Lieferanten bzw. Dienstleister. Gerne gefälscht werden auch E-Mails von Ämtern und Behörden, die dann die Steuerabteilungen erreichen.

MEINE EMPFEHLUNG

Schaffen Sie unbedingt ein Bewusstsein bei Ihren Kollegen dafür, dass sie in einem hochsensiblen Bereich arbeiten. Dieses Bewusstsein ist der erste Schritt dafür, potenzielle Risiken durch Hacker-Angriffe für Ihr Unternehmen zu minimieren.

So kommen Betrüger an Ihre Daten

Sie alle kennen sicherlich die berühmten Spam-Mails, in denen ein ausländischer Prinz – gegen einen entsprechenden Vorschuss zur Deckung seiner Kosten – einen enormen Geldbetrag zu überweisen verspricht. Ebenso weit verbreitet sind zahlreiche E-Mails, in denen Ihnen in schlechtem Deutsch das Blaue vom Himmel versprochen wird, wenn Sie Ihre Bankverbindung angeben.

Führen Sie sich unbedingt vor Augen: Die heutigen Betrugsmaschen sind weitaus professioneller und ausgefeilter. An schlechtem Deutsch werden Sie dank Künstlicher Intelligenz (KI) oder immer besser werdenden Übersetzungsprogrammen kaum noch einen Betrug erkennen. Auch werden Sie in der Regel nicht durch einen vermeintlichen Prinzen und eine skurrile Geschichte mit der Nase auf einen drohenden Betrug gestoßen.

Moderne Cyberkriminelle gehen geschickter vor, um an Ihre Daten und schlussendlich an Ihr Geld zu kommen. Ich habe Ihnen 2 Beispiele aus der „analogen Welt" mitgebracht:

- Ein Paketzusteller steht neben der Eingangstür Ihres Unternehmens, als Sie morgens zur Arbeit kommen. Er fragt nach dem Weg zum Sekretariat und Sie lassen ihn hinein. Statt Pakete abzuliefern sucht er stattdessen nach leeren Büros und fotografiert Unterlagen, die auf den Schreibtischen liegen.
- Gegen Feierabend klingelt bei Ihnen eine Frau, die angibt, als Vertretung von Ihrer Reinigungsfirma geschickt worden zu sein. Da Sie neu in Ihren Räumlichkeiten ist, lässt sie sich zeigen, wo die Reinigungsutensilien aufbewahrt werden. Dann leert sie zunächst die Mülleimer in den Büros der Mitarbeiter, in denen sich unter Umständen auch sensible Unterlagen befinden können.

MEIN TIPP

Das klingt für Sie nach Stoff aus Kriminalromanen? Keineswegs. Laut einer Studie des Branchenverbandes Bitkom werden jedes Jahr rund 22 % der Unternehmen Opfer einer solchen Masche. Man spricht hier auch von analogem Social Engineering. Machen Sie dieses Risiko in Ihrem Unternehmen unbedingt bekannt.

So schützen Sie sich in der analogen Welt

Sie erkennen an den zuvor dargestellten Beispielen, dass es Kriminelle in vielen Fällen viel zu leicht haben, an sensible Daten zu gelangen. Insbesondere durch die folgenden Maßnahmen können Sie Ihr Risiko schnell senken:

- Sperren Sie immer Ihren Bildschirm, wenn Sie den Arbeitsplatz – sei es auch nur kurz – verlassen.
- Lassen Sie keine Unterlagen und Dokumente unbeaufsichtigt auf Ihrem Schreibtisch liegen. Insbesondere die Steuer- und Buchführungsunterlagen sind ein Hauptangriffsziel. Schließen Sie unbedingt die Zimmertür ab, wenn Sie den Raum verlassen.
- Werfen Sie keine Unterlagen mit relevanten Daten in den Mülleimer. Diese sollten stets in einer sogenannten Datentonne entsorgt werden. Hier handelt es sich um einen Mülleimer, in den Sie lediglich Unterlagen einwerfen, aber nicht mehr entnehmen können.
- Externe Datenträger wie USB-Sticks, CDs oder Festplatten dürfen nicht unbeaufsichtigt an Ihrem Arbeitsplatz liegen. Schließen Sie diese idealerweise in einen Schrank ein.
- Holen Sie Ausdrucke direkt aus dem Drucker. Bleiben diese dort unbeaufsichtigt liegen, können die Blätter schnell entwendet oder zumindest eingesehen werden.

Das steckt hinter Social Engineering

Althergebrachte Spam-Mails haben eine Gemeinsamkeit: Sie richten sich an eine breite Masse an Empfängern und sind daher in der Regel sehr allgemein gehalten. Es fehlt die konkrete Ansprache des jeweiligen Empfängers. Zudem wird in der E-Mail auch kein Bezug zu persönlichen Merkmalen des Empfängers hergestellt.

Leider werden Cyberkriminelle immer professioneller. Das zeigt sich insbesondere im sogenannten Social Engineering. Dabei spioniert ein Hacker persönliche Informationen einer bestimmten Person aus. Das Ziel ist klar: Durch eine ganz konkrete Ansprache dieser Person soll ein zielgerichteter Betrugsversuch unternommen werden.

Hier kommen Hacker insbesondere an nützliche Informationen:

- Auf Portalen wie LinkedIn oder Xing werden Angaben zu Unternehmen, Position und Arbeitskollegen eingesammelt.
- Auf vielen Unternehmens-Internetseiten werden Mitarbeiter mit Ihrer Position und Ihrer E-Mail-Adresse benannt.
- Über soziale Netzwerke wie Facebook oder Instagram können persönliche Daten eingesehen werden.

Ein Cyberkrimineller sammelt all diese Daten und kombiniert Sie zu einem Profil. Die so gewonnen Erkenntnisse können dann genutzt werden, um etwa zielgerichtete Phishing-Attacken auszuführen.

So schützen Sie sich in der digitalen Welt

Soziale Netzwerke gehören mittlerweile zu unserem Alltag und wir hinterlassen in ihnen eine Vielzahl an digitalen Fußabdrücken. Damit sind insbesondere Daten gemeint, die im Zweifel ein Cyberkrimineller gegen uns verwenden kann. Die folgenden Tipps kann ich Ihnen an die Hand geben, um es den Kriminellen so schwer wie möglich zu machen:

- Geben Sie nur die notwendigsten persönlichen Informationen preis. Je mehr Sie offenbaren, desto größere Chancen haben Betrüger.
- Seien Sie besonders vorsichtig bei betrieblichen Informationen. Diese haben insbesondere auf Ihren privaten Social-Media-Profilen nichts zu suchen.
- Beschränken Sie die Sichtbarkeit Ihrer preisgegebenen Informationen. In nahezu allen Netzwerken ist es möglich, diese auf eigene Kontakte zu begrenzen.

MEINE EMPFEHLUNG

Sprechen Sie dieses Thema unternehmensintern an und machen Sie klare Vorgaben an Ihre Mitarbeiter, wie diese mit betrieblichen Daten und Informationen zu verfahren haben. Sie können zwar keine Vorgaben zur Nutzung Sozialer Netzwerke machen, allerdings können Sie sehr wohl für drohende Gefahren sensibilisieren.

Wie Sie Cyberattacken abwehren

Ein kurzer Selbsttest. Würden Sie auf den folgenden Link klicken?

„Sehr geehrter Bankkunde, bitte aktualisieren Sie Ihre Daten. Folgen Sie dazu diesem Link. Herzliche Grüße, Kundenservice“

Ich gehe davon aus, dass Sie diesen plumpen Versuch sofort erkennen würden. Anders sieht es aber vielleicht bei dem folgenden Text aus:

„Sehr geehrter Herr Haase, wir haben eine gravierende Sicherheitslücke entdeckt, von der Ihr Bankkonto bei der Sparkasse Dortmund unmittelbar betroffen sein könnte. Sichern Sie sich daher unbedingt schnellstmöglich ab und aktualisieren Sie hier Ihre Daten, bevor Sie Opfer eines Hacker-Angriffs werden. Es grüßt Sie Ihre Sparkasse Dortmund, Filiale Borussiastraße.“

Der zweite Text ist raffinierter gehalten und spricht wichtige menschliche Emotionen und Verhaltensweisen an: Angst, Neugier, Folgsamkeit und Hilfsbereitschaft. Zudem wird ein Druck aufgebaut, dem der Empfänger nachgeben soll. Zudem sind Informationen eingestreut, die einen konkreten Bezug zum Empfänger herstellen.

Auch in dem folgenden Beispiel geht es um Phishing und einen Betrugsversuch:

„Liebe Kolleginnen und Kollegen, in der vergangenen Vorstandssitzung wurde beschlossen, ab sofort eine neue Software auf allen Geräten zu installieren, die im Hintergrund läuft und eine stabilere Internetverbindung gewährleistet. Laden Sie sich dazu umgehend die Datei über diesen Link herunter. Herzliche Grüße, Ihr Vorstandsvorsitzender Richard Rentrop.“

An den Beispielen erkennen Sie deutlich, dass es nicht reicht, eine E-Mail nur zu überfliegen und den Anweisungen zu folgen. Sie müssen stets misstrauisch werden, wenn diese

- einen Link oder Anhang enthalten,
- zu einer Handlung auffordern,
- Belohnungen versprechen oder
- in irgendeiner anderen Art seltsam erscheinen.

MEIN TIPP

Auch an dieser Stelle müssen Sie Aufklärungsarbeit betreiben. Zahlreiche Mitarbeiter würden sicherlich der Aufforderung des Vorstandsvorsitzenden uneingeschränkt Folge leisten. Machen Sie allen Kollegen klar, dass E-Mails leicht zu fälschen sind.

Woran Sie gefälschte E-Mails erkennen

Wären Sie auf die E-Mail der Sparkasse oder des Vorstandsvorsitzenden hereingefallen? Es gibt noch weitere Wege, gefälschte E-Mail-Nachrichten zu entlarven:

- Achten Sie auf die Absenderdetails: Zwar zeigen viele E-Mail-Programme standardmäßig nur den Absendernamen (Beispiel: „Timm Haase“) an. Bewegen Sie den Mauszeiger über den Namen, ohne darauf zu klicken, wird Ihnen aber die Absenderadresse (Beispiel: „Betrugsversuch@hackenleichtgemacht.com“) angezeigt. Die Fälschung dieser Adresse ist sehr aufwendig, sodass Hacker auf diesen Schritt oftmals verzichten.
- Prüfen Sie die Links: Bewegen Sie die Maus über einen Link, wird Ihnen die URL, also die Internetadresse, angezeigt, auf die der Link verweist. Achten Sie hier insbesondere auf Rechtschreibfehler, die Ähnlichkeit zu bekannten Adressen suggerieren sollen.
- Nehmen Sie persönlichen Kontakt auf: Sind Sie sich nicht sicher, ob hinter einer E-Mail ein Phishing-Versuch steckt? Dann gehen Sie auf Nummer sicher und nehmen Sie persönlich Kontakt zu dem Absender auf. Natürlich sollten Sie dazu nicht auf die E-Mail antworten oder die in der Nachricht angegebene Telefonnummer verwenden.

ACHTUNG

Eine weitere Masche des Social Engineerings: Sie finden auf dem Firmenparkplatz einen USB-Stick. Was liegt näher, als diesen sofort auf seinen Inhalt hin zu überprüfen? Hier soll die menschliche Neugier ausgenutzt werden. Leider sind Sie in dem Moment, in dem der Stick in Ihrem Rechner steckt, bereits Opfer eines Hackers geworden und Ihr Computer kann infiziert sein.