Phishing und trojanische Pferde - Angriffe auf den eigenen PC erkennen und abwehren

I. Unerwartete E-Mails: nur ärgerlich oder eine Gefahr?

Warum unerwartete E-Mails gefährlich sein können

Nicht nur der heimische Briefkasten ist oft mit Werbung verstopft, auch der elektronische Briefkasten wird immer mehr zugemüllt. Solche unerwarteten und unbestellten E-Mails werden umgangssprachlich auch als Spam bezeichnet. Während Sie Werbung im heimischen Briefkasten alternativ zur direkten Entsorgung in der Regel gefahrlos öffnen können, müssen Sie in der digitalen Welt die nötige Portion Misstrauen an den Tag legen. Denn in der digitalen Welt begegnen Ihnen Spam, Viren, trojanische Pferde, Phishing, Pharming und viele andere Gefahren, vor denen Sie sich auf jeden Fall schützen müssen.

Die drei wichtigsten Regeln im Umgang mit unerwarteten Mails lauten:

- **Klicken Sie niemals auf Links.**
- **Öffnen Sie niemals Datei-Anhänge.**
- **Antworten Sie nicht auf diese Mails.**

Wenn Sie diese drei Regeln beherzigen, haben Sie die größte Gefahrenquelle im Umgang mit unerwarteten E-Mails schon ausgeschaltet. Haben Sie eine Mail als Betrugsversuch entlarvt, löschen Sie diese. Aber bitte leiten Sie die E-Mail vor dem Löschen an phishing@vz-nrw.de und – wenn möglich – zusätzlich an den echten Anbieter weiter. Denken Sie an Ihre Mitbürger, die solche E-Mails nicht als Betrug erkennen. Mit der Weiterleitung helfen Sie, vor solchen kriminellen Machenschaften zu warnen und ermöglichen zusätzlich die schnellere Sperrung betrügerischer Internetseiten.

Welche Arten von Spam gibt es?

Spam, also unerwartete elektronische Post, gibt es in ganz verschiedenen Formen. Häufig verbreitet sind folgende Varianten:

- **Phishing:** Jemand gibt sich als Absender eines tatsächlich existierenden Unternehmens aus – beispielsweise eine Bank, ein Kreditkartenunternehmen oder ein Zahlungsdienstleister – und versucht, Sie zur Eingabe von persönlichen Daten zu bewe-

gen. In der Regel geschieht dies über einen in der E-Mail hinterlegten Link, der Sie zu einer nachgebauten Internetseite des in der Mail genannten Unternehmens führt. Aber auch der Einsatz eines Datei-Anhangs im html-Format ist möglich. Gelingt den Tätern das Vorhaben, haben sie Zugriff auf Ihr Online-Banking-Konto.

- **Trojanisches Pferd:** Im Gegensatz zum Phishing wollen die Absender der E-Mail Sie hier nicht dazu bewegen, Ihre Daten auf einer vorbereiteten Seite einzutragen. Sie wollen Sie vielmehr dazu bringen, einen mitgelieferten Datei-Anhang – oft im zip-Format - zu öffnen. In diesem ist ein Schadprogramm enthalten, beispielsweise ein Virus oder ein trojanisches Pferd. Einmal installiert, verschafft das Programm den Kriminellen Zugang zum Computer. Umgangssprachlich hat es sich etabliert, bei dieser Form der Internetkriminalität nicht von trojanischen Pferden, sondern von Trojanern zu sprechen. Wirklich korrekt ist das aber nicht – schließlich waren Trojaner die Einwohner von Troja und damit Opfer des Tricks mit dem hölzernen Pferd. Daher verwenden wir im weiteren Verlauf den in der Sache korrekten Begriff: trojanisches Pferd.
- **Geldversprechen:** Wer träumt nicht heimlich von einer reichen Erbschaft? Oder davon, für vergleichsweise wenig Arbeit viel Geld zu verdienen? Oder von einer Idee, wie man schnell an Vermögen kommt? Die vermeintliche Erfüllung dieser Träume kommt oft per unerwarteter E-Mail. Hier spielen die Kriminellen aber nicht die gute Fee, sondern wollen in der Regel stattdessen erst an Ihre persönlichen Daten und dann an Ihr Geld kommen. Im schlimmsten Fall wollen die Kriminellen Sie gar für illegale Geldwäschen oder sonstige dunkle Geschäfte missbrauchen. Wenn Sie sich auf so etwas einlassen, machen Sie sich strafbar und haben am Ende noch Polizei und Staatsanwaltschaft im Haus. Ihre Mittäter sind dann aber schon über alle Berge.
- **Werbung:** Wenn man Ihnen ungefragt echte oder vermeintliche Schnäppchen anbietet, Ihnen Glücksspiele ans Herz legt oder Mitgliedschaften anbietet, ist das oft ärgerlich – aber als einzige Spam-Form letztlich wenig gefährlich.

II. Phishing

Was ist Phishing eigentlich?

Phishing setzt sich aus dem englischen Begriff für Passwort-Fischen zusammen. Das Bundesamt für Sicherheit in der Informationstechnik (https://www.bsi.de) erläutert den Begriff wie folgt:

„Phishing ist ein Kunstwort aus "Passwort" und "Fishing" und bezeichnet Angriffe, bei denen Benutzern gezielt Passwörter, Kreditkartendaten oder andere vertrauliche Informationen entlockt werden. Hierzu werden häufig Methoden des Social Engineering, teilweise in Verbindung mit Identitätsdiebstahl, verwendet. Beispielsweise können die Angreifer geschickt formulierte E-Mails an die Benutzer senden.“

Den Kriminellen geht es also darum, Sie dazu zu bringen, persönliche Daten wie beispielsweise PIN, Girokontonummer oder Kreditkartennummer preiszugeben. Die Phishing-E-Mail wird dazu so konstruiert, dass sie Vertrauen schafft und den Eindruck erweckt, von einem echten Anbieter zu stammen. Meistens arbeiten die Kriminellen mit einem Link, der Sie zu einer Seite mit einer Eingabemaske für persönliche Daten führt.

Wie ist eine Phishing-Mail grundsätzlich aufgebaut?

Jeden Tag werden viele unterschiedliche Varianten von Phishing-E-Mails versendet. Auch wenn diese in äußerer Form und inhaltlichem Text verschieden sind, gibt es doch übereinstimmende Merkmale im Aufbau der Mail:

- **Die Anrede:** Bei vielen Phishing-Mails steht eine allgemeine Anrede wie „*Sehr geehrter Kunde*“ oder „*Sehr geehrte Damen und Herren*“. Immer häufiger werden die E-Mail-Empfänger aber auch persönlich mit Vor- und Zunamen angesprochen.
- **Der Grund der E-Mail:** Nach der Anrede erfährt der E-Mail-Empfänger, warum diese Mail verschickt wird. Hier verfügen die Kriminellen über einen bunten Strauß an erfundenen Gründen. Beliebt sind zum Beispiel Gesetzesänderungen, die Einführung einer neuen Sicherheitstechnik oder Unstimmigkeiten im Kundenkonto, die geklärt werden müssen.
- **Die Notwendigkeit zum Handeln:** Nachdem der Grund für die Versendung der E-Mail erklärt wurde, geht es jetzt darum, dass der E-Mail-Empfänger aktiv werden muss. In der Regel soll er seine Daten erneut eingeben, kontrollieren, bestätigen oder verifizieren.
- **Der Zeitdruck:** Damit die E-Mail-Empfänger nicht zu lange nachdenken können und am Ende doch noch misstrauisch werden, gibt es nur eine kurze Zeitspanne für das vermeintlich notwendige Handeln. Dies können beispielsweise 48 Stunden, sieben Tage oder das Ende des laufenden Monats sein.
- **Die Konsequenzen des Nichthandelns:** Wer nicht innerhalb dieser kurzen Frist aktiv wird, dem werden schwere Konsequenzen angedroht. Oft geht es darum, dass ein

Konto eingeschränkt wird, gar nicht mehr genutzt werden kann oder sogar aufgelöst wird.

- **Link oder Anhang:** Die Kriminellen fügen der E-Mail einen Link oder einen Datei-Anhang bei. In wenigen Ausnahmefällen geht es darum, dass eine Antwort per E-Mail erbeten wird. Der angebotene Weg, entweder auf den Link zu klicken oder den Anhang zu öffnen, wird als einfache und kostenlose Lösung, als zwingend notwendig oder als Service verkauft.

Bei **E-Mails mit trojanischen Pferden** – umgangssprachlich wird hier oft von Trojanern gesprochen – ist der Aufbau weitgehend identisch. Unterschiede sind eher inhaltlicher Art, insbesondere beim Grund, warum die E-Mail verschickt wird, und den Konsequenzen des Nichthandelns. Als Grund wird oft ein erfundener Kauf, eine vermeintliche Bestellung, eine fiktive Mitgliedschaft oder eine angebliche Mahnung angegeben. Der E-Mail-Empfänger wird aufgefordert, endlich einen noch offen stehenden Betrag zu begleichen. Die Daten finde man im Anhang. Alternativ geht es auch darum, dass man den Anhang öffnen müsse, um die Daten zu kontrollieren oder gar sein Widerrufsrecht auszuüben. Wer nicht innerhalb einer kurzen Frist aktiv wird, dem wird mit einem Rechtsanwalt, einer gerichtlichen Klage oder einem Inkassobüro gedroht. Bei dieser Form der Internetkriminalität fügen die Absender einen Datei-Anhang bei. Dieser Anhang erscheint oft im zip-Format und enthält ein Schadprogramm. Grundsätzlich muss es die Datei aber nicht zwangsweise auf „zip“ enden, Schadprogramme können sich auch hinter anderen Formaten wir zum Beispiel rar verbergen.

An welchen Merkmalen können Sie Phishing-E-Mails erkennen?

Auch heute noch gibt es viele eher schlecht gemachte Phishing-E-Mails, die sich oft durch eines oder mehrere der folgenden Kriterien auszeichnen:

- Eine allgemeine Anrede wie „Liebe Kunden“ oder „Sehr geehrte Damen und Herren“. Ein Anbieter, bei dem Sie tatsächlich Kunde sind, wird Sie persönlich ansprechen. Leider ist umgekehrt eine persönliche Anrede keine Garantie, dass die E-Mail echt ist, sondern nur ein Indiz, dass sie möglicherweise echt sein könnte.

- Die E-Mail ist nicht in deutscher Sprache geschrieben, sondern in der Regel in englischer Sprache verfasst. Warum sollte Sie ein deutscher Anbieter in einer fremden Sprache anschreiben?

- Die E-Mail wurde mit Hilfe eines Computerprogramms ins Deutsche übersetzt. Der Text ist gekennzeichnet durch eine ganze Reihe von Tippfehlern, von Sätzen, die keinen Sinn ergeben und von einzelnen Wörtern, die gar nicht übersetzt wurden –

weil schon im englischen Original ein Tippfehler vorlag. Eine solche E-Mail würde ein echter deutscher Anbieter nie verschicken.

Es gibt aber auch Phishing-E-Mails, die professionell gestaltet sind, die nicht die oben genannten Merkmale aufweisen und daher deutlich gefährlicher sind. Es gibt eine persönliche Anrede und keine grammatikalischen Fehler. Aber auch bei diesem Fall existieren Kriterien, die Ihnen helfen, die E-Mail als Betrugsversuch zu entlarven:

- Wenn Sie tatsächlich Kunde bei diesem Unternehmen sind, dieser Anbieter Sie aber sonst nicht per E-Mail kontaktiert, ist die Wahrscheinlichkeit besonders hoch, dass die E-Mail nicht echt ist. Wenn Sie bei diesem Anbieter gar nicht Kunde sind, gilt dies erst recht.

- Sie finden den im Punkt „**Wie ist eine Phishing-Mail grundsätzlich aufgebaut?“** geschilderten Aufbau vollständig oder zumindest weitgehend wieder.

- Die Absenderadresse ist gefälscht. Die Adresse, die zu sehen ist, stimmt nicht mit der Adresse überein, die im Header steht.
  (Hinweis: Was der Header ist und wie Sie diesen einsehen können, erläutert die Verbraucherzentrale auf https://www.vz-nrw.de/phishing).

- Die Internetadresse, die im Text angegeben ist, stimmt nicht mit der Internetadresse überein, zu der der Link tatsächlich führt. Dies können Sie leicht herausfinden: Gehen Sie mit der Maus auf den Link, **ohne auf diesen zu klicken** – auf dem Bildschirm wird angezeigt, wo der Link tatsächlich hinführt.

Wer ist von Phishing betroffen?

Wenn Sie eine Phishing-E-Mail erhalten, können Sie sicher sein, dass diese nicht nur an Sie gegangen ist. Die Kriminellen versenden solche Mails massenhaft über entsprechende Verteiler. Im Vorfeld haben sie unzählige E-Mails gesammelt und schicken die Mail dann einfach an alle im Verteiler vorhandenen E-Mail-Adressen. Kreditkartenbesitzer bekommen solche E-Mails genauso wie Verbraucher, die gar keine Kreditkarte besitzen. In anderen Fällen bekommen Verbraucher Phishing-E-Mails einer bestimmten Bank, obwohl sie dort gar kein Kunde sind.

Wenn Sie also eine Phishing-E-Mail im Namen eines Anbieters erhalten, bei dem Sie tatsächlich Kunde sind, bedeutet das also nicht zwangsläufig, das Sie zielgerichtet angeschrie-

ben wurden oder gar ein Datenleck beim echten Anbieter vorliegt. Oft ist es schlicht Zufall – bei irgendjemanden müssen die Kriminellen schließlich einen „Treffer“ landen, wenn die E-Mail an so viele Verbraucher verschickt wird. Und wenn am Ende ein kleiner Promillesatz auf die Phishing-E-Mail hereinfällt, reicht das den Kriminellen offenkundig.

Auch bei den Unternehmen und Institutionen, deren Namen sie missbrauchen, sind die Kriminellen nicht wählerisch, wenn sie Phishing-E-Mails oder E-Mails mit trojanischen Pferden im Anhang verschicken. Banken sind genauso betroffen wie Kreditkartenunternehmen, Online-Zahlungsdienste, E-Mail-Provider, Geschäfte im Groß- und Einzelhandel und so weiter und so fort.

Die Liste der betroffenen Unternehmen reicht von Sparkassen über Mastercard bis hin zu PayPal, Telekom, Lidl und Real, von der Postbank über Commerzbank, Deutsche Bank, Visacard bis hin zu Amazon, Ebay, Tchibo und dem Anbieter des Spiels World of Warcraft, also Blizzard. Die Kriminellen sind sogar so dreist, dass einige betrügerische E-Mails im Namen eines Bundes- oder Landesministeriums oder einer sonstigen nationalen oder internationalen öffentlichen Institution geschrieben werden.

Sie haben eine Phishing-E-Mail als Betrug erkannt – reicht es, die E-Mail zu löschen?

Es ist das zweitbeste Szenario, dass Sie eine Phishing-E-Mail als Betrug erkennen und sofort löschen. Das beste Szenario besteht darin, die Mail vor dem Löschen an

phishing@vz-nrw.de

und – wenn möglich – auch an den echten Anbieter weiterzuleiten. Denken Sie daran, dass nicht alle Ihre Mitmenschen den Betrugsversuch als solchen erkennen. Helfen Sie anderen Verbrauchern dadurch, dass Sie die E-Mail vor dem Löschen weiterleiten. Die E-Mail-Adresse phishing@vz-nrw.de ist so konzipiert, dass die Annahme nicht verweigert wird. Falls Sie beim Versuch, eine Mail an das Phishing-Radar weiterzuleiten, eine Fehlermeldung bekommen, liegt dies wahrscheinlich an Ihren Sicherheitseinstellungen. Ihr System hat die E-Mail, was eigentlich zu begrüßen ist, als Betrugsversuch identifiziert und verhindert den Versand. In dem Fall können Sie versuchen, uns den reinen Text der E-Mail ohne Anhänge und Links zu senden.

Die Verbraucherzentrale führt seit Dezember 2010 das sogenannte Phishing-Radar und stellt diese E-Mails anonymisiert in ein speziell eingerichtetes Phishing-Forum ein, welches Sie über die Adresse

https://www.vz-nrw.de/phishing

erreichen können. Zusätzlich prüft die Verbraucherzentrale bei Phishing-E-Mails, die einen Link enthalten, ob noch die enthaltene betrügerische Seite gesperrt werden muss. Die sodann gesperrten Seiten und die darauf verlinkenden Phishing-E-Mails können umso weniger finanziellen Schaden bei Verbrauchern verursachen, je eher sie gesperrt werden. Genau hier können Sie mithelfen: Durch die Weiterleitung der Mail an phishing@vz-nrw.de und – wenn möglich – an den echten Anbieter. Das Phishing-Radar warnt täglich auf der Seite „Phishing-Radar: aktuelle Warnungen“ sowie über Twitter (https://twitter.com/vznrw_finanzen) über aktuelle Betrugsmaschen.

III. Links in Phishing-E-Mails

Warum sollten Sie Links, die in einer E-Mail mitgeschickt werden, nicht vertrauen?

Die Antwort lautet schlicht: Solange Sie nicht sicher sein können, dass die E-Mail tatsächlich von einem echten Anbieter – beispielsweise Ihrer Hausbank – stammt, solange dürfen Sie einem Link in dieser Mail nicht vertrauen. Das Problem ist: Solange sich elektronische Signaturen nicht durchgesetzt haben und jeder Verbraucher auch weiß, wie er damit die Echtheit einer E-Mail überprüfen kann, kann jeder Absender einer E-Mail gefälscht sein und Ihnen auf diesem Wege einen geschickt gefälschten Link zukommen lassen.

Natürlich verschicken auch die echten Anbieter E-Mails an ihre Kunden, so dass die Frage, ob die E-Mail nicht doch echt sein könnte, nicht unberechtigt ist. In Ausnahmefällen kommt es sogar vor, dass in einer seriösen E-Mail ein Link enthalten ist. Ein Anbieter führt neue Allgemeine Geschäftsbedingungen (AGBs) ein und verlinkt auf diese. Oder er weist die Kun-

den auf eine laufende Aktion hin. Früher haben einige Banken sogar den Zugang zu ihrer Webseite als Service-Link ihren E-Mails beigefügt.

Links in E-Mails von echten Anbietern sind aber die große Ausnahme. Der Grund ist recht simpel: Es ist wiederholt vorgekommen, dass die Kriminellen auf die Verfassung von eigenen, kreativen Texten verzichten und einfach den Text des echten Anbieters kopieren – und dann nur die Adresse austauschen, zu der der Link führt. Immer mehr Anbieter haben diese Gefahr inzwischen erkannt und verzichten deshalb darauf, in eigenen E-Mails überhaupt noch mit Links zu arbeiten. So wird eine Bank Sie im Zweifel lediglich darauf hinweisen, dass Sie sich wie gewohnt in Ihr Konto einloggen sollen, aber keinen Link beifügen. Wenn eine E-Mail einen Link enthält, sollten bei Ihnen sofort die Alarmglocken schrillen.

Warum ist bereits das Klicken auf einen Link gefährlich, wenn es doch an der Stelle noch gar nicht um die Eingabe persönlicher Daten geht?

Schadprogramme wie ein trojanisches Pferd können Sie sich einfangen, wenn Sie einen Datei-Anhang öffnen. Dies ist aber nicht der einzige Weg, auf dem Sie ungewollt Ihren Computer infizieren können. Andere Gefahrenquellen sind externe Geräte wie USB-Sticks, aber auch das Surfen im Internet. Auf präparierten Internetseiten, aber auch auf geknackten und infizierten Webseiten von seriösen Anbietern kann im Quellcode ein Schadprogramm enthalten sein. Dieses sucht gezielt nach einer Schwachstelle Ihres Computers. Findet es eine solche Schwachstelle, beispielsweise im Internetbrowser oder im Betriebssystem, installiert sich das Schadprogramm. Diese Methode nennt man auch „Drive-by-Download“. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bezeichnet diese Vorgehensweise wie folgt: „*Dieses Vorgehen gleicht einem Einbrecher, der nacheinander Türen und Fenster auf Schwachstellen untersucht, um möglichst schnell und unauffällig ins Haus zu gelangen.*“

Beim Öffnen eines Dateianhangs müssen Sie als Nutzer also erst noch selbst aktiv werden, damit die Kriminellen Erfolg haben – um im Bild zu bleiben, also freiwillig einen Fremden ins Haus lassen. Beim „Drive-by-Download“ öffnen Sie dagegen – eine Schwachstelle in Ihrem Computer vorausgesetzt – Kriminellen Tür und Tor, ohne selbst aktiv zu werden und ohne es überhaupt zu bemerken. Daher ist es ganz wichtig, den Virenschutz, den Internetbrowser und das Betriebssystem stets auf dem neuesten Stand zu halten, um genau dieses Szenario zu vermeiden. Auch eine Firewall hilft, unerlaubte Netzwerkzugriffe zu unterbinden. Zu Hause achten Sie ja auch darauf, dass Türen und Fenster stets verschlossen sind, damit niemand Unbefugtes eindringen kann. Gleiches sollte für Ihren Computer gelten.

Nicht auf allen betrügerischen Internetseiten, auf die in unerwarteten E-Mails verlinkt wird, sind im Quellcode solche Schadprogramme enthalten. Oft geht es den Kriminellen tatsächlich „nur“ darum, dass die Nutzer auf diesen Seiten persönliche Daten wie PIN, Girokontonummer oder Kreditkartennummer preisgeben sollen. Wenn Sie an dieser Stelle misstrauisch werden und die Seite verlassen, ohne Daten eingegeben zu haben, endet die Sache oft noch einmal glimpflich.

Woran können Sie eine betrügerische Internetseite erkennen?

Wenn Ihr Browser in der Adresszeile vermeintlich die Adresse Ihrer Hausbank zeigt, ist auch das leider **kein** verlässliches Zeichen, dass Sie sich auch tatsächlich auf deren Internetseite befinden. Besonders gefährlich sind Links, die im Browserfenster lange kryptische Anhänge enthalten, wie man dies gewohnt ist, wenn man sich bei der Bank eingewählt hat. Egal wie lang der Link und wie die Kolonne aus Zahlen und Buchstaben konstruiert ist: Das Entscheidende ist der Beginn der Internetadresse, zu der der Link führt – auf diesen müssen Sie Ihre Aufmerksamkeit richten.

Oft unterscheidet sich der Beginn der Betrugsseite von der Seite des echten Anbieters lediglich durch eine auf den ersten Blick schlecht zu erkennende absichtliche Änderung im Namen, also eine Art „Tippfehler“, oder durch einen oft sogar gut klingenden und damit Vertrauen bildenden Zusatz. Nachfolgend zeigen wir einige fiktive Beispiele. Der Zusatz „...“ steht für eine beliebige nachfolgende Kolonne von Zahlen und Buchstaben:

Echter Anbieter	**Betrugsseite mit „Tippfehler“**	**Betrugsseite mit Zusatz**
https://www.paypal.com/...	http://www.paipalll.com/...	http://www.paypal-anmelden.com/...
http://www.visa.de/...	http://www.vjisa.de/...	http://www.visa-sicherheit.de/...
http://www.mastercard.com/...	http://www.masterrcard.com/...	http://www.konfliktloesen-mastercard.com.eu/...
https://www.deutsche-bank.de/...	http://www.deutsche-bamk.de/...	http://www.123abc.www.deutsche-bank.de.ru/...
http://www.amazon.de/...	http://www.amazson.de/...	http://www.amazon-richtlinien.de.pl/...

Alternativ nutzen die Kriminellen auch Seiten, in deren Internetadresse der Name des echten Anbieters gar nicht erst vorkommt. Dies vereinfacht es Ihnen, den Betrug als solchen zu erkennen. Beispiele hierfür sind: http://hamischbrewn.com/wp-includes/Tex/ oder http://bairosflinkai.eu/Index/.

Was ist der Unterschied zwischen einer http-Seite und einer https-Seite?

Die korrekte Internetadresse des echten Anbieters, auf der Kunden persönliche Daten eingeben sollen, beginnt immer mit http**s**:// und nicht mit http://. Dieser eine Buchstabe, das „**s**“, besitzt eine große Bedeutung. Es ist – bildlich gesehen – bei der Kommunikation der Übergang von einer Postkarte, die jeder lesen kann, hin zum verschlossenen Briefumschlag. Dritte können also nur noch sehen, wer an wen schreibt, aber nicht mehr den Inhalt mitlesen. Seriöse Anbieter arbeiten an Stellen, an denen persönliche Daten eingegeben werden, aus Sicherheitsgründen immer mit einer https://-Seite. Kriminelle arbeiten dagegen in der Regel mit einer http://-Seite – also ohne das „s“. Sie scheuen den Aufwand, den eine https://-Seite mit sich bringt. Denn diese muss – siehe nachfolgender Absatz – zertifiziert werden. Auf einer http://-Seite sollten Sie daher niemals persönliche Daten eintragen. Oder würden Sie Ihre PIN auf eine Postkarte schreiben und diese in den Briefkasten werfen? Richtigerweise wohl nicht. Die gleiche Einstellung müssen Sie auch an den Tag legen, wenn Sie im Internet unterwegs sind.

Sie erkennen eine so geschützte Verbindung an der Zeichenfolge http**s**://www.name-der-bank.de in der Adresse (also dem Zusatz s bei http) bzw. an einem Symbol mit einem Schloss oder einem ähnlichen Symbol (variiert je nach dem Browserprogramm) in der Statusleiste. In der Regel können Sie sich über dieses Symbol das Zertifikat anzeigen lassen. Dort können Sie überprüfen, ob dieser Seitenschlüssel wirklich für Ihren Anbieter ausgestellt wurde. Jedes Zertifikat ist wiederum mit einem Zertifikat abgesichert. Das Zertifikat am Ende ist in der Regel mit dem Browser oder Betriebssystem mitgeliefert und stammt von großen wichtigen Zertifizierungsstellen. Durch diese mehrfache Absicherung soll sichergestellt werden, dass ein Betrüger sich nicht selbst ein Zertifikat ausstellen kann. Der Name der Internetseite, für die das Zertifikat ausgestellt ist, darf nicht nur ähnlich klingen, sondern muss absolut identisch mit der Seite sein, die Sie anwählen wollten. Denn jeder Täter könnte sich bei anerkannten Zertifizierungsstellen ein solches Zertifikat auf einen ähnlich klingenden Namen ausstellen lassen, aber eben nicht für die Originalseite der Bank, auf die er nicht registriert sein kann. Bei der sicheren Internetverbindung werden alle übermittelten Daten so

verschlüsselt, dass nur der richtige Empfänger sie entschlüsseln und nutzen kann (Stichwort: verschlossener Briefumschlag).

Anmerkung: Die Startseite eines echten Anbieters muss nicht zwangsläufig bereits eine https://-Seite sein. Spätestens, wenn persönliche Daten abgefragt werden, wechseln seriöse Anbieter aber auf diese sichere https://-Seite.

IV. Handlungsempfehlungen und Sicherheitshinweise

Welche Sicherheitshinweise sollten Sie beachten?

Wo Gefahren lauern, sollte man gewisse grundsätzliche Regeln beachten, um Schadensfälle so gut es geht zu vermeiden. Als Fußgänger schauen Sie ja auch nach links und rechts, bevor Sie eine Straße überqueren. Dadurch verringern Sie beträchtlich das Risiko, von einem PKW erfasst zu werden.

Die gleiche Sorgfalt sollten Sie auch an den Tag legen, wenn Sie im Internet unterwegs sind. Eigentlich muss die Sorgfalt sogar noch höher sein. Denn im Internet tummeln sich leider viele zwielichtige Gestalten, die Sie absichtlich schädigen wollen. Und der potentielle Schädiger kann im Internet irgendwo auf der Welt sitzen, während im Straßenverkehr nur die PKW relevant sind, die gerade die Straße entlangfahren, die Sie überqueren wollen.

Die drei wichtigsten Regeln im Umgang mit unerwarteten E-Mails hatten wir bereits auf Seite eins erläutert. Da diese unglaublich wichtig sind, wiederholen wir sie an dieser Stelle:

- **Klicken Sie niemals auf Links.**
- **Öffnen Sie niemals Datei-Anhänge.**
- **Antworten Sie nicht auf diese Mails.**

Im Detail empfehlen wir Ihnen, folgendes zu beachten:

- Leiten Sie betrügerische E-Mails an phishing@vz-nrw.de und – wenn möglich – auch an den echten Anbieter weiter. Sie helfen damit, andere Verbraucher zu warnen und betrügerische Seiten zu sperren.
- Halten Sie das Virenschutzprogramm, den Internetbrowser und das Betriebssystem stets auf dem aktuellen Stand. Prüfen Sie auch, ob die Sicherheitsprogramme stets

automatische Updates durchführen. Auch eine Firewall hilft, unerlaubte Netzwerkzugriffe zu unterbinden.

- Geben Sie die Internetadresse zu Ihrer Bank immer selbst per Hand ein.
- Vertrauen Sie keinen Linklisten oder Angaben auf Internetseiten Dritter.
- Gehen Sie mit persönlichen Daten im Internet sehr sparsam um. Je freigiebiger Sie diese preisgeben, um so größer ist die Gefahr, dass Ihre Daten in einen Verteiler geraten, den Kriminelle nutzen.
- Fragen Sie bei Ihrem E-Mail-Provider nach, wie Sie die Einstellungen in Ihrem Spam-Filter optimieren können, damit unerwünschte elektronische Post im Vorfeld als solche erkannt wird und gar nicht erst Ihr Postfach erreicht.
- Wenn Ihr Postfach trotzdem unzumutbar zugemüllt wird, löschen Sie die E-Mail, die in einen Verteiler geraten ist und eröffnen Sie eine neue. Nutzen Sie mehrere E-Mail-Adressen, damit nicht alle Bereiche Ihres Lebens betroffen sind, wenn Sie eine E-Mail-Adresse löschen müssen. Idealerweise nutzen Sie für das Online-Banking eine separate E-Mail-Adresse, die nur Ihre Bank kennt. Wenn Sie eine E-Mail erreicht, die angeblich von Ihrer Bank stammen soll, haben Sie ein weiteres Prüfkriterium. Sie prüfen, ob die Mail an die korrekte, nur der Bank bekannten E-Mail-Adresse gesendet wurde, oder an eine ganz andere E-Mail-Adresse, die Ihnen zwar gehört, die Sie aber gar nicht für Bankzwecke nutzen.
- Schauen Sie regelmäßig in Ihre Kontounterlagen. Misstrauen Sie aber auch im Zweifel Postzusendungen, die Sie erhalten und eine Ihnen nicht bereits bekannte Adresse enthalten. Prüfen Sie genau, ob diese Post wirklich von Ihrer Hausbank stammt.
- Ihre Bank wird von Ihnen niemals die Angabe von PIN, TAN oder anderen persönlichen Daten zu Kontrollzwecken verlangen. Nutzen Sie beide Angaben nur für die Kontobewegungen auf der von Ihnen angesurften Webseite. Zeigen Sie im Übrigen immer ein notwendiges Maß an Misstrauen.
- Sichern Sie wichtige Daten auf einer externen Festplatte.
- Ändern Sie in regelmäßigen Abständen Passwörter und Sicherheitsfragen. Achten Sie darauf, dass Ihr Passwort aus wenigstens acht Zeichen besteht, die Großbuchstaben, Kleinbuchstaben, Zahlen und mindestens ein Sonderzeichen beinhalten, so dass Dritte dieses nicht erraten können.

- Trauen Sie niemals mitgesandten Links oder Datei-Anhängen. **ABSOLUT NIEMALS!** Ignorieren Sie diese E-Mails stattdessen.

Bitte bedenken Sie: Eine hundertprozentige Sicherheit wird es im Internet, insbesondere beim Online-Banking, nie geben. Wenn Sie die Sicherheitshinweise beachten, ist aber die Wahrscheinlichkeit, dass Sie Opfer von Kriminellen werden, deutlich reduziert.

Bedeutung der Sicherheitshinweise: Was könnte ein Schadprogramm verursachen?

Mit der Installation eines Schadprogramms wollen Kriminelle letztlich an Ihr Geld. Der Weg dorthin ist aber durchaus unterschiedlich. Wenn sich ein Schadprogramm einmal installiert hat, sind ganz unterschiedliche Szenarien denkbar. Nachfolgend einige – tatsächlich schon passierte – Beispiele:

- Das Schadprogramm sucht den gesamten Rechner nach Passwörtern und Zugangsdaten ab und sendet diese an die Kriminellen.
- Zukünftig wird jede Tastatureingabe protokolliert und an die Kriminellen versandt.
- Die Kriminellen klauen Ihre Identitäten, beispielsweise in sozialen Netzwerken.
- Das Programm lotst Sie auf ganz andere Internetseiten und nicht auf die Seiten, auf die Sie eigentlich gelangen wollten. Sie machen eigentlich alles richtig, geben also die echte Internetadresse Ihrer Bank per Hand ein, aber das Schadprogramm manipuliert die Eingabe und führt Sie stattdessen auf eine nachgebaute Betrugsseite. Dieses Vorgehen nennt man Pharming.
- Wenn die Kriminellen im Besitz Ihrer PIN sind, stellen sie Ihr Online-Banking auf ein anderes Verfahren um, fangen den Bestätigungsbrief der Bank ab und räumen dann das Konto leer.
- Die PIN ermöglicht es den Kriminellen auch, Ihre Kontobewegungen nachzuvollziehen. Sie wissen, bei welchen Unternehmen Sie Kunde sind und können Sie zukünftig zielgerichtet anschreiben – sogar mit richtiger Kundennummer.
- Alle Ihre Bekannten und Freunde, die in Ihrem Kontaktbuch stehen, erhalten eine E-Mail. Darin steht, dass Sie angeblich alleine in einer ausländischen Stadt sind, Ihnen gerade alles gestohlen wurde und Sie schnellstmöglich Geld brauchen. Wie eine schnelle und unkomplizierte Überweisung möglich ist, wird natürlich auch angegeben.

Dies ist nur eine kleine Auswahl dessen, was für Kriminelle möglich ist, wenn sie die Kontrolle über Ihren Computer übernommen haben. Wie Sie sehen, ist nichts davon erstrebenswert. Umso wichtiger ist es, von vorneherein zu verhindern, dass sich überhaupt ein Schadprogramm auf Ihrem Computer installiert.

Ist eine Reaktion auf die E-Mail nicht doch sinnvoll?

Eine unerwartet eingehende E-Mail versetzt vor allem Verbrauchern einen Schreck, die noch keine oder nur wenig Erfahrung im Umgang mit Phishing und trojanischen Pferden haben. Gerade dann ist die Sorge groß, ob eine Reaktion auf die Mail nicht doch nötig ist. Sei es, um die angedrohte Sperrung des Kontos zu verhindern, einen Kaufvertrag noch rechtzeitig zu widerrufen oder etwas anderes Wichtiges zu tun.

Jetzt ist es entscheidend, nicht vorschnell zu handeln. Denn genau darauf setzen die Kriminellen – dass Sie im ersten Schreck den Anhang öffnen oder auf einer präparierten Seite Daten eingeben. Das wäre aber der größte Fehler, den Sie an der Stelle überhaupt machen können.

Wenn Sie zu dem im Text genannten Unternehmen keine vertragliche Verpflichtung eingegangen sind, können Sie die Mail bedenkenlos in den digitalen Mülleimer verschieben – idealerweise leiten Sie diese aber vorher an **phishing@vz-nrw.de** und, wenn möglich, an den echten Anbieter weiter.

Sind Sie – was vorkommen kann – tatsächlich eine Vertragsbeziehung zu dem in der E-Mail genannten Unternehmen eingegangen und wollen sich vergewissern, ob der Inhalt nicht doch echt ist, dann spricht grundsätzlich nichts dagegen, den echten Anbieter zu kontaktieren. **Aber tun Sie das keinesfalls, indem Sie auf die E-Mail antworten oder eine in der E-Mail genannte Kontaktmöglichkeit nutzen.** Wenn möglich, gehen Sie in eine Filiale des Anbieters und fragen Sie dort nach. Ist das nicht möglich, finden Sie eine Kontaktmöglichkeit auf der echten Internetseite des Anbieters.

Antworten Sie keinesfalls auf die Mail selbst. Denn was würde passieren, wenn Sie es täten? Wenn Sie „Glück“ haben, haben die Betrüger die Phishing-E-Mail von der E-Mail-Adresse eines arglosen Verbrauchers verschickt. Dieser kann mit Ihrer Antwort-E-Mail herzlich wenig anfangen, da er für den Versand ja gar nicht verantwortlich war und selbst ein Opfer ist. Wenn Sie „Pech“ haben, antworten Sie aber tatsächlich den Kriminellen. Dann bestätigen Sie mit Ihrer Antwort nicht nur die Echtheit der E-Mail-Adresse und die Tatsache, dass die

Adresse regelmäßig abgerufen wird, sondern geben schlimmstenfalls noch – absichtlich oder versehentlich – weitere persönliche Daten preis.

Sie sehen daran übrigens auch, dass es bei einer einzigen Phishing-E-Mail drei Opfer geben kann:

- Sie als Empfänger der E-Mail.
- Das Unternehmen oder die Institution, dessen/deren Name missbraucht wird.
- Der Absender der E-Mail, der ein argloser Verbraucher sein kann, dessen Account missbraucht wird.

Was tun im Schadensfall?

Im Schadensfall gilt unsere Empfehlung, bei unerwarteten Mails nicht vorschnell zu handeln, nicht mehr. Das Gegenteil ist jetzt richtig. Wenn Sie auf Kriminelle reingefallen sind, müssen Sie, um (weiteren) Schaden zu vermeiden, folgende zwei Dinge beachten: **Handeln Sie schnell und zeigen Sie keine falsche Scham**. Sie sind nicht der Erste, der auf solch einen miesen Trick hereingefallen ist und Sie werden auch nicht der Letzte sein. Denn wenn keiner darauf hereinfallen würde, könnten sich die Betrüger diese E-Mails ja sparen. Konkret sollten Sie folgendes tun:

- Sperren Sie sofort die betroffenen Konten und Karten. Kontaktieren Sie daher als allererstes Ihre(n) Anbieter.
- Aktualisieren Sie sofort das Antivirenprogramm, das Sie verwenden und lassen Sie es nach der Aktualisierung den gesamten Computer überprüfen. Bei vielen Antiviren-software-Anbietern gibt es grundsätzlich auch die Möglichkeit, einen Online-Scan durchführen zu lassen. Informieren Sie sich hier auf der Homepage des Anbieters Ihrer Antivirensoftware, fragen Sie gegebenenfalls per E-Mail nach. Schließlich bleibt Ihnen noch die Möglichkeit, sich an einen Fachmann zu wenden, der den Rechner vor Ort überprüft.
- Sollten Sie mehr als einen Computer haben, arbeiten Sie mit einem nicht betroffenen Rechner. Nutzen Sie den befallenen Rechner nicht, bevor dieser wieder sicher ist.
- Ändern Sie Passwörter und Sicherheitsfragen. Achten Sie darauf, dass Ihr Passwort aus wenigstens acht Zeichen besteht, die Großbuchstaben, Kleinbuchstaben, Zahlen und mindestens ein Sonderzeichen beinhalten, sodass Dritte dieses nicht erraten können.

- Informieren Sie gegebenenfalls auch Ihre Freunde, Bekannten und Geschäftspartner, falls die Gefahr besteht, das ein Dritter Mails in Ihrem Namen versendet. Damit helfen Sie mit, Betrugsversuche zu vereiteln.
- Erstatten Sie Strafanzeige bei der Polizei. Löschen Sie in diesem Fall keineswegs die E-Mails, auf die Sie hereingefallen sind, da diese ein Beweismittel sind. Falls Sie diese bereits gelöscht haben, schauen Sie nach, ob sie noch im Papierkorb zu finden sind.

Anmerkung: Unsere Empfehlung von Seite eins, Phishing-E-Mails nach der Weiterleitung an phishing@vz-nrw.de und – wenn möglich – an den echten Anbieter zu löschen, gilt ausschließlich für den Fall, dass Sie den Betrugsversuch erkennen. Wenn Sie allerdings auf einen Betrugsversuch hereinfallen, bedeutet dies aber, dass Sie den Betrug nicht erkannt und die E-Mail im Vorfeld nicht gelöscht haben. Dann dürfen Sie die E-Mail im Nachhinein auch nicht mehr löschen, da diese dann ein wichtiges Beweismittel ist.

Wo bekommen Sie weitere Informationen oder technische Hilfe?

Abhängig von der Art der Frage können Ihnen folgende Ansprechpartner helfen:

- Die Verbraucherzentralen unter https://www.vz-nrw.de/phishing. Dort und auf https://twitter.com/vznrw_finanzen finden Sie die aktuellen Phishing-Warnungen.
- Das Bundesamt für Sicherheit in der Informationstechnik:

  https://www.bsi.de oder www.bsi-fuer-buerger.de
- Landeskriminalämter und sonstige Polizeidienststellen:

  Zum Beispiel www.polizei-beratung.de oder www.polizei.nrw.de
- Ihr E-Mail-Provider.
- Bei technischen Fragen bekommen Sie Hilfe auf den Internetseiten einschlägiger Fachzeitschriften.

