Schneller und ohne Sperren: Alternative DNS-Server einsetzen

DNS-Server lösen Namen zu IP-Adressen auf und sind essenziell fürs Surfen. Wer nicht die Standard-Server der Provider nutzt, surft schneller und ohne Blockaden.

Schneller und ohne Sperren: Alternative DNS-Server einsetzen

DNS-Server lösen Namen zu IP-Adressen auf und sind essenziell fürs Surfen. Wer nicht die Standard-Server der Provider nutzt, surft schneller und ohne Blockaden.

Bevor ein Browser eine Internetseite anfragen kann, muss er die Adresse, die der Nutzer eingetippt hat, erst auflösen – über das Domain Name System, kurz DNS. Ein DNS-Server

funktioniert wie ein Adressbuch, in dem ein Name wie heise.de einer IP-Adresse zugeordnet ist. Ohne zügige Namensauflösung ist zügiges Surfen also nicht möglich.

In einem typischen Heimnetzwerk ist der primäre DNS-Server für die Geräte der Router – doch der kennt nicht alle IP-Adressen der Welt. Bekommt er eine Frage, die er nicht beantworten kann, reicht er die Frage an einen öffentlichen DNS weiter. Wer nichts weiter unternimmt und den Router nach Anweisungen seines Internetanbieters eingerichtet hat, nutzt als öffentlichen DNS-Server einen Dienst des Providers. Doch es gibt Alternativen und gute Gründe, einen anderen DNS-Server als den des Providers einzutragen.

Netzsperren

Die DNS-Server von deutschen Providern liefern nicht immer die Wahrheit, die im DNS hinterlegt ist. Bei Internetseiten, deren hauptsächliches Ziel es ist, urheberrechtlich geschütztes Material widerrechtlich zu verbreiten (vor allem Filme, Livesport und Musik), leiten die DNS-Server die Anfragen auf eine Seite der „Clearingstelle Urheberrecht im Internet“ (CUII) um. Die Juristen der CUII nennen solche Seiten „strukturell urheberrechtsverletzend“. Kritiker befürchten seit der Einführung solcher Netzsperren, dass sie auch für Zensur unliebsamer Inhalte genutzt werden könnten. Die Seiten sind aber gar nicht wirklich gesperrt – der Provider-DNS verrät nur einfach nicht die richtige Adresse.

Ende März 2023 bewies Provider 1&1, wie gefährlich Manipulationen am DNS sein können. Durch einen technischen Fehler landete die Adresse heise.de bei einigen Nutzern auf der Liste für CUII-Sperren. Statt des Newstickers sahen sie eine Sperrseite. Der Fehler wurde schnell beseitigt, beweist aber, dass fälschliche Sperren kein theoretisches Problem sind.

Wer mit solchen Sperren und potenzieller Zensur nichts zu tun

haben will, greift zu einem alternativen DNS-Anbieter aus dem Ausland, dort hat die CUII keinen Einfluss. Doch es geht auch andersherum: Einige alternative DNS-Server haben bewusst eigene Netzsperren eingebaut. Sie filtern zum Beispiel für Kinder ungeeignete Inhalte oder Adressen, die im Zusammenhang mit Schadsoftware aufgefallen sind. In Umgebungen mit Kindern (zu Hause oder zum Beispiel in der Schule) kann das sinnvoll sein. Welcher Anbieter für Sie infrage kommt, lesen Sie im Abschnitt „Alternativen“.

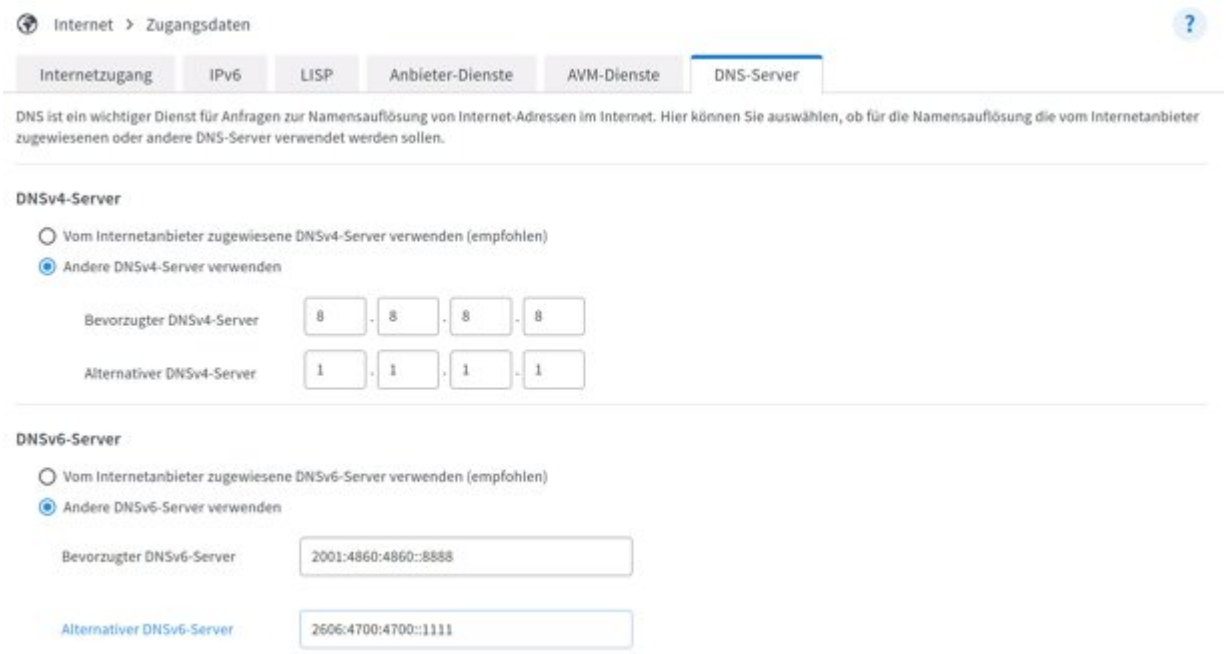
Geschwindigkeit

Die Namensauflösung per DNS ist für die gefühlte Internetgeschwindigkeit mindestens so wichtig wie die Auslieferung der Daten selbst. Eine Gedenksekunde vorm Besuchen einer Website braucht niemand. Und bei der Geschwindigkeit sind die Provider-DNS-Server nicht gerade Spitzenklasse. Zwar sind Messungen von DNS-Geschwindigkeiten immer mit Vorsicht zu genießen und fast jeder der alternativen Anbieter sagt über sich, dass er am schnellsten auflösen kann. Die Erfahrung zeigt aber: DNS-Anbieter wie Google, Quad9 und Cloudflare (dazu später mehr) lösen im Schnitt schneller auf als die Server der Provider. Besonders in Stoßzeiten holt man mit einem solchen Anbieter etwas Geschwindigkeit heraus.

So geht es

Den DNS-Anbieter fürs eigene Netz zu wechseln, ist in wenigen Minuten erledigt und funktioniert fast in jedem Router gleich. Suchen müssen Sie nach einem Punkt, der Interneteinstellungen heißt. Dort gibt es meist einen Haken, um die Standard-Server des Providers zu nutzen, darunter zwei Felder für eigene IP-Adressen. Der Hintergrund: Fällt mal ein Server aus, greift der Router zum zweiten. Sie bekommen davon gar nichts mit. Eine sinnvolle Strategie kann es sein, als zweiten Server eine Adresse eines anderen Anbieters zu nutzen. Das reduziert die Wahrscheinlichkeit für Ausfälle ungemein.

In der in Deutschland verbreiteten Fritzbox finden Sie die Einstellung unter dem Menüpunkt Internet/Zugangsdaten/DNS-Server.



Schnell geändert: In der Fritzbox stellt man den DNS-Server für das Heimnetz unter Internet/Zugangsdaten/DNS-Server um.

Alternativen

Den Markt mit alternativen DNS-Servern aufgemischt hat Google, indem das Unternehmen die sehr leicht zu merkenden Adressen 8.8.8.8 und 8.8.4.4 für DNS-Server eingesetzt haben. Wie immer bei Google gilt: Das Angebot ist solide und sehr schnell, im Gegenzug muss man aber damit leben, dass Google die Nutzung protokolliert und analysiert.

Nach Google stieg ein anderes US-Unternehmen ins Rennen ein: Cloudflare bietet für Unternehmen zahlreiche kommerzielle Dienstleistungen im Netz an, kostenlos sind seine DNS-Server unter den Adressen 1.1.1.1 und 1.0.0.1. Cloudflare selbst gibt an, dass es keine Logs anfertigt, wer welche Seiten aufgelöst hat. Von Cloudflare gibt es noch zwei weitere Angebote: 1.1.1.2 (und 1.0.0.2 als Reserve) filtern Malware-verbreitende Seiten. 1.1.1.3 (und 1.0.0.3) filtern Malware und Erwachseneninhalte.

Eine europäische Alternative ist Quad9, betrieben von einer Stiftung aus der Schweiz. Deren IP-Adresse lautet 9.9.9.9 (und 149.112.112.112 als Reserve). Ebenfalls aus Europa kommt das Projekt DNS.Watch mit der IP-Adresse 84.200.69.80 (und 84.200.70.40 als Reserve). Eine Rechtsform hat das Projekt nicht, auch die Macher treten nicht in Erscheinung – offenbar Schutzmaßnahmen, um nicht zu Sperren wie die durch die CUII gezwungen werden zu können.

Anbieter	Sitz	Erste IPv4	Alternative IPv4	Erste IPv6	Alternative IPv6
Cloudflare	USA	1.1.1.1	1.0.0.1	2606:4700:4700::1111	2606:4700:4700::1001
Google	USA	8.8.8.8	8.8.4.4	2001:4860:4860::8888	2001:4860:4860::8844
Quad9	Schweiz	9.9.9.9	149.112.112.112	2620:fe::fe	2620:fe::9
DNS.WATCH	Deutschland	84.200.69.80	84.200.70.40	2001:1608:10:25::1c04:b12f	2001:1608:10:25::9249:d69b

In der Tabelle sehen Sie die Adressen der DNS-Anbieter in der Übersicht. Wenn Sie per IPv6 surfen und Ihr Router auch Felder für IPv6-DNS-Server hat, finden Sie die passenden Adressen in den letzten beiden Spalten.

Sicherheitsforscher Sönke Huster über Lücken im WLAN-Stack des Linux-Kernels

„Es reicht, wenn du dein WLAN anhast“

Über die Luft gehackt werden, nur weil das WLAN eingeschaltet ist? Im August hat Sönke Huster Sicherheitslücken im WLAN-Stack des Linux-Kernels gefunden, die einen solchen Angriff theoretisch ermöglicht hätten. Seine Entdeckung zeigt, wie wichtig es ist, Software ausführlich zu testen.
Über die Luft gehackt werden, nur weil das WLAN eingeschaltet ist? Im August hat Sönke Huster Sicherheitslücken im WLAN-Stack des Linux-Kernels gefunden, die einen solchen Angriff theoretisch ermöglicht hätten. Seine Entdeckung zeigt, wie wichtig es ist, Software ausführlich zu testen.

Von Kathrin Stoll

Sönke Huster ist wissenschaftlicher Mitarbeiter am Secure Mobile Networking Lab (SEEMOO) der TU Darmstadt. Im August 2022 hat er fünf Sicherheitslücken im WLAN-Stack des Linux-

Kernels entdeckt. Mittlerweile gibt es Patches. Wir haben mit ihm über den Fund, seine Methodik und den Disclosure-Prozess gesprochen.

Der Sicherheitsforscher Sönke Huster hat fünf Sicherheitslücken im Linux-Kernel gefunden. Wie er das gemacht hat, verrät er im Gespräch mit c’t. *Josephine Franz*

c’t: Wie kommt man darauf, im Linux-Kernel nach Sicherheitslücken zu suchen?

Sönke Huster: Ich habe dieses Jahr meine Masterthesis über Bluetooth-Fuzzing unter Linux geschrieben. Die Idee kam von meiner Masterarbeitsbetreuerin Dr. Jiska Classen. Im Bluetooth-Stack habe ich dann auch ein paar kleine Sicherheitslücken gefunden. Dann wurde ich wissenschaftlicher Mitarbeiter am Secure Mobile Networking Lab von Prof. Matthias

Hollick und es lag nahe, es auf WLAN auszuweiten. Aus Angreifersicht sind WLAN und Bluetooth super interessant und auch irgendwie ähnlich. Wenn ich dich hacken will, ist es ja viel cooler, ich kann das durch die Luft aus dem Raum nebenan machen, ohne dass ich dafür erst physisch auf deinen Rechner zugreifen können muss, um zum Beispiel einen USB-Stick einzustecken. Beide Protokolle sind dafür prädestiniert.

c't: Du hast gleich fünf Lücken im Linux-Kernel gefunden. Wie bist du dabei vorgegangen?

Huster: Die Methode, die ich verwende, heißt Fuzzing. Sie wurde in den Achtzigerjahren von Barton Miller [Professor der Informatik in Madison, Wisconsin, Anm. d. Red.] entdeckt, der sich über eine Telefonleitung auf Holzmasten remote auf seinem Arbeitsrechner einloggte. Bei Gewitter wurde die Übertragung des Signals gestört und seine Eingaben kamen verzerrt an. Das führte dazu, dass Programme abstürzten oder sich anders verhielten als erwartet. So kam man dahinter, dass man zufällige Eingaben nutzen kann, um Bugs und Sicherheitslücken zu finden und das Fuzzing – auch Fuzz-Testing – war erfunden. Heute verwendet man dazu sogenannte Fuzzer. Das sind im Grunde Programme, die die Eingabeschnittstellen von Programmen, Betriebssystemen oder Netzwerken mit zufälligen Daten fluten.

Mit komplett zufälligen Eingaben arbeitet man heute aber nicht mehr. Man kann das Verfahren verfeinern und Eingaben benutzen, die nah an denen sind, die das Target – in diesem Fall eben Linux in meiner VM – erwartet. Um WLAN zu untersuchen, lasse ich den Fuzzer WLAN-Pakete mit kleinen Anomalien an das Linux-System in meiner virtuellen Maschine schicken, die er fortlaufend verändert. Dabei beobachtet und dokumentiert der Fuzzer, welcher Code im Kernel zur Verarbeitung der mutierten WLAN-Pakete getriggert wird. Man könnte auch sagen: welchen Weg ein Paket bei der Verarbeitung nimmt. Immer, wenn bei der Verarbeitung eines Pakets Code abgedeckt wurde, der vorher noch nicht ausgeführt wurde, nimmt der Fuzzer dieses Paket in sein Eingabeset auf und nutzt es als Ausgangspunkt für neue

Mutationen. Diese veränderten Pakete schickt er dann wieder an den Kernel. Das Ganze passiert ein paar Tausend Mal pro Sekunde. Das Ziel ist es, möglichst viel Code „zu covern“, also durch die mutierten Eingaben Teile des Kernel-Codes abzudecken, die der Fuzzer noch nicht kennt. Coverage-Guided Mutational Fuzzing lautet der Fachbegriff für diese Art von Fuzz-Testing.

c’t: Wenn das Target abstürzt, hat man einen Treffer gelandet?

Huster: Genau. Ein Absturz oder anderes unerwartetes Verhalten, zum Beispiel, wenn es sich aufhängt, sind eigentlich immer ein Hinweis auf einen Bug oder eine Schwachstelle. Die Eingaben, die so etwas bewirken, speichert der Fuzzer separat ab, sodass ich den Crash reproduzieren kann. Bei einer der fünf Lücken, die ich gefunden habe, war es zum Beispiel so, dass ein kaputtes Paket – oder eine Reihe von Paketen – eine sogenannte Linked List korrumpierte und quasi das letzte Paket in der Liste wieder auf das erste gezeigt hat. Bei der Verarbeitung wusste das Betriebssystem nie, wann die Liste zu Ende ist und hat sich schließlich aufgehängt, weil es aus dieser Schleife nicht rauskam.

c’t: Das klingt nach einem ärgerlichen Bug, aber nicht nach einem, den ein Angreifer für eine Remote Code Execution nutzen könnte.

Huster: Nein. Es wäre schwierig, eine Möglichkeit zu finden, das auszunutzen. Die Endlosschleife führt dazu, dass das Betriebssystem sich aufhängt und das wars. Aber eine andere der Lücken ermöglicht es einem Angreifer, den Speicher zu überschreiben, sodass er theoretisch Code aus der Ferne ausführen könnte. Der Kernel reserviert Speicher für die Ausführung von Programmen und Prozessen. Wenn jetzt beispielsweise 128 Byte an einer Stelle im Speicher für einen bestimmten Vorgang vorgesehen sind, dann darf man da eigentlich auch nicht mehr als diese 128 Byte reinschreiben. Bestimmte Eingaben des Fuzzers haben Fehler in der

Paketverarbeitung aufgedeckt, die dazu führen, dass man mehr als die vorgesehene Länge in einen für einen Vorgang reservierten Teil des Speichers schreiben kann – ein sogenannter Buffer Overflow.

c't: Das wäre bereits ausreichend, damit ein Angreifer einen Rechner aus der Ferne übernehmen könnte?

Huster: Theoretisch. Es war möglich, als Angreifer 256 Byte kontrolliert in den Speicherbereich zu schreiben, der auf den zugewiesenen folgte. Für eine RCE müsste man zusätzlich herausfinden, wo im Speicher die kaputten WLAN-Pakete, die diesen Fehler im Kernel-Code triggern, überhaupt verarbeitet werden. Das ist aber gar nicht so einfach, weil es Mechanismen gibt, die dafür sorgen, dass der Kernel immer an unterschiedlichen Stellen im Speicher ausgeführt wird. Kernel Address Space Layout Randomization nennt sich das. Aber es wäre denkbar, dass sich noch weitere Sicherheitslücken finden, die einem das verraten.

c't: Ist das eine Hypothese oder hast du das auch erfolgreich prüfen können?

Huster: Nein. Das übersteigt meine Fähigkeiten. Es ist schon eher eine Hypothese. Aber eine, die sehr wahrscheinlich zutrifft. Es gibt verschiedene Arten von Sicherheitslücken und eine Lücke von diesem Typ bietet sich – in diesem konkreten Fall eben in Kombination mit weiteren – theoretisch dafür an.

Aus Angreifersicht das Spannende an den Sicherheitslücken ist, dass man überhaupt keine Nutzerinteraktion braucht. Du musst dich nicht aus Versehen mit einem Hotspot verbinden, den der Hacker kontrolliert, damit er dir böse WLAN-Pakete schicken kann. Es reicht, wenn du dein WLAN anhast und dein Gerät nach Netzwerken in der Umgebung sucht. Im Hintergrund passiert das relativ häufig zur Standortbestimmung. Es ist nicht wie bei einem Phishing-Versuch, bei dem der Angreifer das Opfer erst dazu bringen muss, auf einen Button zu klicken und Login-Daten

einzugeben. Genau das macht solche Lücken potenziell so kritisch. Linux-Nutzer gibt es nicht so viele, aber drei der Lücken betreffen Android, und Android-Nutzer gibt es eine ganze Menge. Am Smartphone haben die meisten Nutzer ihr WLAN in der Regel an.

c’t: Ist der Fuzzer eine Eigenentwicklung des Secure Mobile Networking Labs?

Huster: Ja. Wir nutzen Komponenten aus LibAFL. Das ist eine Bibliothek, die ein sehr gutes Grundgerüst mitbringt, aber die Architektur unseres Fuzzers unterscheidet sich stark von der bestehender Fuzzer.

c’t: Kannst du sicher sein, dass es außer den fünf Lücken nicht noch weitere gibt?

Huster: Ich denke, man kann auf jeden Fall sagen, dass WLAN unter Linux durch unsere Arbeit ein bisschen sicherer geworden ist. Wir waren an Stellen im Kernel, wo meines Wissens nach noch nicht so viel gefuzzt wurde. Momentan gucken wir uns noch weitere Teile an und bisher haben wir nichts weiter gefunden. Aber hundertprozentige Sicherheit, dass es nicht noch mehr Bugs und Sicherheitslücken gibt, wird man nie haben. Es kann immer unvorhergesehene Eingaben geben, die einen Bug oder eine Sicherheitslücke offenlegen. Ein Angreifer kann sie genauso gut finden wie wir. Genau deshalb ist Fuzz-Testing so wichtig.

c’t: Seit Oktober gibt es Patches. Wie und an wen hast du die Sicherheitslücken gemeldet?

Huster: Es gibt gefühlt 1000 Anlaufstellen für Linux-Sicherheitssachen, zum Beispiel eine Mailing-Liste aller Hersteller irgendwelcher Linux-Distributionen. Dort hätte ich das melden können. Parallel hätte ich dann noch die Kernel-Leute informieren müssen. Ich hab mich entschieden, den Prozess an einen Hersteller abzugeben und habe mich an SUSE gewandt. Die SUSE-Leute haben Johannes Berg von Intel ins Boot geholt. Er ist der Maintainer des WLAN-Stacks unter Linux. Für

mich war es superspannend, mit ihm in so einem engen Austausch zu stehen, während er die Patches für die beiden Sicherheitslücken, die ich initial an SUSE gemeldet hatte, geschrieben hat.

Er hat mir die Patches dann geschickt und ich habe meinen Fuzzer darauf angesetzt. So sind wir auf die drei weiteren Sicherheitslücken – und insgesamt noch ein paar weitere kleinere Bugs – gestoßen. Das Ganze hat ein paar Wochen gedauert. Als alle Patches fertig waren, hat SUSE alle anderen Hersteller im Geheimen informiert und man hat einen Zeitpunkt festgelegt, zu dem man die Öffentlichkeit über die Lücken informiert. Die Hersteller hatten bis dahin über eine Woche Zeit, entsprechende Updates rauszubringen. Überrascht hat mich, dass manche Hersteller ihre Updates erst mehrere Tage nach der Bekanntgabe der Lücken verteilt haben.

c’t: C gilt als relativ unsichere Programmiersprache. Künftig soll es möglich sein, Kernel-Komponenten stattdessen in Rust zu schreiben. Hätte das deine Sicherheitslücken verhindert?

Huster: Sehr wahrscheinlich wären diese Lücken nicht aufgetreten, hätte man die Module in Rust geschrieben. Gerade die Geschichte, dass man Speicher überschreiben kann. Der Rust-Compiler hätte verhindert, dass die Kernel-Entwickler diesen Fehler überhaupt einbauen. Aber es gibt natürlich auch Fehler, die durch keine Programmiersprache der Welt verhindert werden.

c’t: Gibt es etwas, was du Admins und Anwendern raten würdest?

Huster: Sicherheitsupdates immer schnell einzuspielen. Wie gesagt, bis alle größeren Distributionen die Updates verteilt haben, hat es nach Veröffentlichung noch ein paar Tage gedauert. Gerade bei Android dauert es oft länger. Es kann einfach sein, dass die betreffende Sicherheitslücke schon eine Weile öffentlich ist, bis man als Nutzer ein Sicherheitsupdate bekommt. Deshalb sollte man Updates möglichst sofort

installieren. Auch wenn es nervt. Aber dann holt man sich in der Zwischenzeit halt mal einen Kaffee. (*kst@ct.de*)

Weitere Infos: ct.de/yvwk

Fake-Shops erkennen und Schäden vermeiden

Niemals ausgeliefert

Beim digitalen Einkauf betrügerischen Läden auf den Leim zu gehen, ist ärgerlich und teuer. Mit ein paar Grundregeln und hilfreichen Tools vermeidet man das. Wir stellen sie vor und

erklären, was im Schadensfall noch möglich ist.
Beim digitalen Einkauf betrügerischen Läden auf den Leim zu gehen, ist ärgerlich und teuer. Mit ein paar Grundregeln und hilfreichen Tools vermeidet man das. Wir stellen sie vor und erklären, was im Schadensfall noch möglich ist.

Von Nick Akinci

Über vier Millionen Deutsche sind schon einmal auf einen Fake-Shop hereingefallen. Das schätzt das von der Bundesregierung geförderte Marktbeobachtungsinstitut „Marktwächter digitale Welt“. Besonders häufig bieten solche Shops nach Angaben des Instituts Sportartikel, Elektronik sowie Haushaltsartikel, Bekleidung und Fahrräder, aber auch Brillen und Schmuck.

Wir zeigen, wie Sie Ihnen unbekannte Shops anhand verlässlicher Kriterien und mit hilfreichen Tools auf Seriosität prüfen, wie Sie Zahlungen absichern und was Sie tun können, falls Sie doch auf einen Fake-Shop hereingefallen sind.

Was ist ein Fake-Shop?

Fake-Shops sind Online-Shops, mit denen Kriminelle gutgläubigen Kunden ihr Geld abnehmen wollen, ohne ihnen die versprochene Ware zu liefern. In der einfachsten Variante erhalten Kunden, die darauf hereinfallen, überhaupt keine Ware. Etwas perfidere Betrüger versenden leere Kartons. Im Nachhinein behaupten sie, dass die Ware auf dem Versandweg abhandengekommen sein müsse. Mitunter verschicken sie auch Ware, die in keiner Weise der Produktbeschreibung entspricht.

Viele Fake-Shops sind nur für einen relativ kurzen Zeitraum online, da sie fast immer auffliegen und der Hoster sie im besten Fall vom Netz nimmt. In diesem Zeitfenster versuchen die Betrüger, möglichst viel Geld zu ergaunern. Sitzt der Hoster im Ausland, können sich solche Shops auch über Jahre halten.

Prüfender Blick

Fake-Shops sind häufig nicht auf den ersten Blick als solche zu erkennen. In Zeiten von Baukastensystemen wie Shopify & Co. klicken Betrüger professionell aussehende Online-Shops in wenigen Stunden zusammen. Es gibt jedoch eine Reihe von Indizien, die für einen Fake-Shop sprechen.

Um Kunden anzulocken, bieten die Täter die Ware in Fake-Shops oft deutlich günstiger an als in anderen Online-Shops. Insbesondere beliebte und häufig gehandelte Markenware preisen sie unter dem Marktwert an, gern als Sonderangebot getarnt. Schnäppchenjäger können sich auf Preisvergleichsseiten einen Eindruck verschaffen, ob die Preisgestaltung realistisch ist.

Als Nächstes schaut man in das Impressum. Fake-Shops haben oft keines, obwohl dies in Deutschland gesetzliche Pflicht ist – die Betrüger wollen ihre Identität verschleiern. Aber Achtung: Manche Fake-Shops enthalten ein echt aussehendes Impressum, welches jedoch schlicht falsche, unvollständige oder von anderen Websites kopierte Angaben enthält. Ob die Firma an der angegebenen Adresse sitzt, kontrolliert man am besten mit Google Maps. Den Unternehmensnamen und die zugehörige Handelsregisternummer prüft man auf handelsregister.de [1].

Abgesehen vom Impressum fehlen in vielen Fake-Shops auch Telefonnummern oder E-Mail-Adressen, um Kontakt aufzunehmen. Ebenfalls kein gutes Zeichen ist es, wenn sich Kontaktmöglichkeiten beschränken auf ausschließlich Handy- oder kostenpflichtige Nummern, Postfachadressen oder lediglich ein Kontaktformular. Misstrauen ist geboten, wenn AGB und Datenschutzerklärung sowie Widerrufsbelehrungen und Versandbedingungen fehlen.

Gütesiegel sind ein Hinweis auf vertrauenswürdige Shops, doch in Fake-Shops trifft man immer wieder einfach hineinkopierte oder frei erfundene Varianten an. Letztere ähneln teils bekannten Gütesiegeln – wie etwa dem von Trusted Shops.

Verfügt der Online-Shop über ein Gütesiegel, kann man auf der Homepage der Organisation prüfen, ob es sich um ein tatsächlich anerkanntes Gütesiegel handelt und ob der Online-Shop es rechtmäßig erworben hat. Durch einen Klick auf das Siegelsymbol muss man auf die Seite der dahinterstehenden Organisation gelangen. Verbreitet und vertrauenswürdig ist außer Trusted Shops auch das EHI Retail Institute („Geprüfter Online-Shop“). Als zuverlässig gilt außerdem das in Kopenhagen ansässige Bewertungsportal Trustpilot (alle unter ct.de/yu3d).

Kein Impressum, kein Handelsregistereintrag, keine Umsatzsteuer-ID, Shop ganz neu, Google Maps kennt den Shop an der angegebenen Adresse nicht und als Kontaktmöglichkeit nur eine Mobiltelefonnummer: Hier heißt es Finger weg!

Zahlmethoden

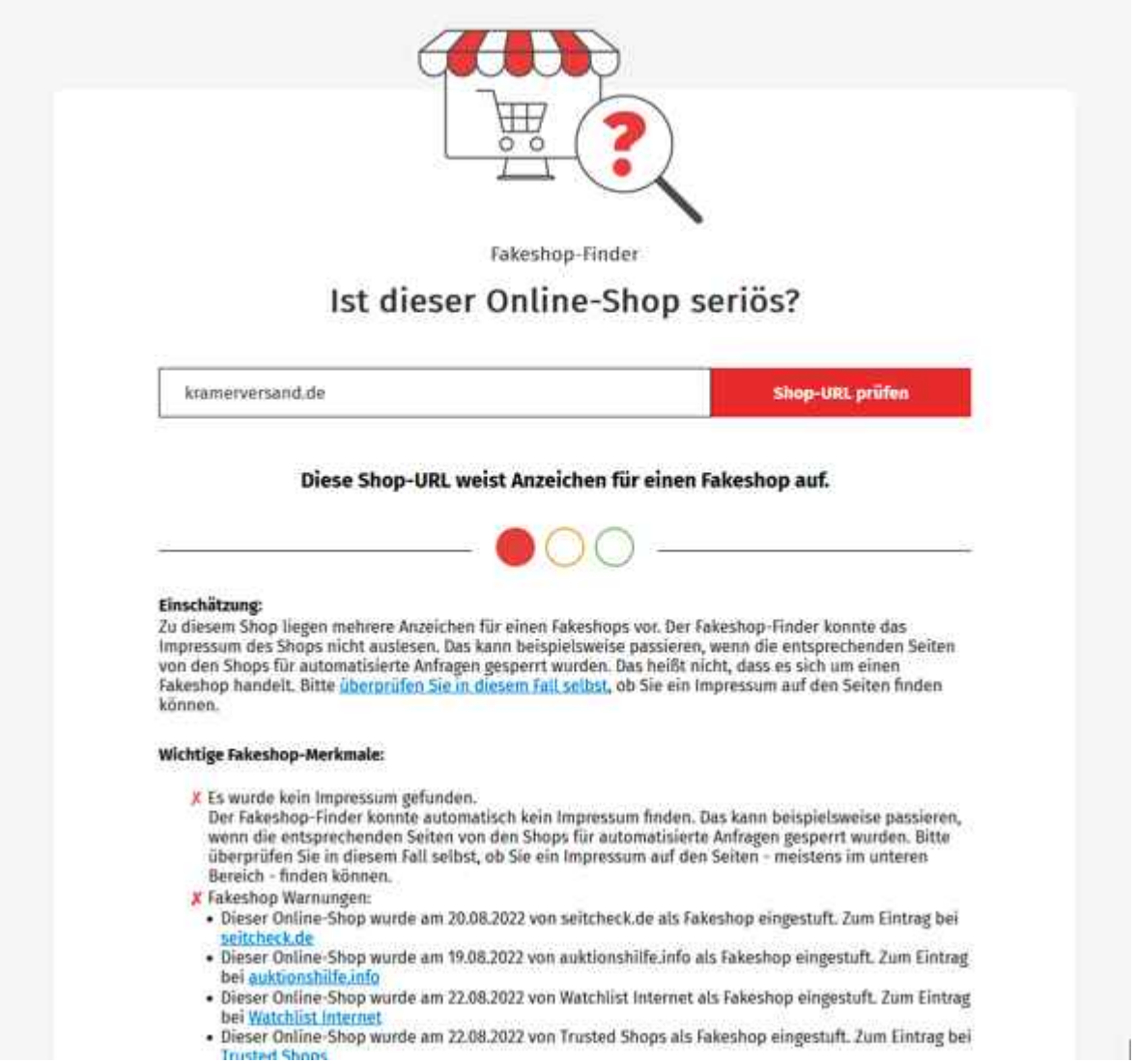
Als Zahlart bieten viele Fake-Shops ausschließlich Vorkasse per Banküberweisung an, da man solche Zahlungen in der Regel nicht rückgängig machen kann. Mitunter wollen betrügerische Händler Kunden auch gerne zu PayPal-Zahlungen in der Variante „Freunde und Familie“ verleiten. Die beinhalten aber im Unterschied zur Option „Waren und Dienstleistungen“ keinen Käuferschutz. Manchmal bietet der Fake-Shop auch zum Schein weitere Zahlarten an, um Vertrauen zu schaffen. Die

funktionieren dann aber aus vorgeschobenen Gründen nicht. Daraufhin bitten die Täter um Vorkasse oder die unsichere PayPal-Variante.

Auch bei vermeintlich sicheren Bezahlmethoden gibt es Haken. Der PayPal-Käuferschutz ist zum Beispiel an Bedingungen wie Paketversand mit elektronischer Sendungsverfolgung geknüpft [3]. Ähnlich halten es Amazon oder Klarna. Manche Betreiber von Fake-Shops schicken die Pakete daher an Adressen von Strohleuten, um Kunden über die Sendungsverfolgung erst in Sicherheit zu wiegen und anschließend Käuferschutzverfahren zu erschweren. Mehr zu Vor- und Nachteilen von Zahlarten haben wir unter [2] zusammengetragen.

Blacklists und Prüftools

Bleibt man unsicher, helfen Tools von Verbraucherschützern und anderen Organisationen. Zunächst lohnt sich ein Blick auf Blacklists. Hierbei handelt es sich um Listen von Online-Shops, die bereits als Fake-Shops eingestuft oder die mehrfach als solche gemeldet worden sind. Solche Listen finden sich zum Beispiel auf der Website der Verbraucherzentrale Hamburg, der Präsenz des Siegel-Anbieters Trusted Shops oder auf der Watchlist Internet. Der Fake-Shop-Kalender der Verbraucherzentrale Bundesverband macht zusätzlich auf zeitweise besonders häufig betroffene Branchen aufmerksam (alle Seiten unter ct.de/yu3d). Darüber hinaus kann sich der Besuch der Preisvergleichsseiten Geizhals und Idealo lohnen (Hinweis: Geizhals gehört wie c’t zu Heise Medien). Sie listen nur geprüfte Online-Shops sowie Händler auf Marktplätzen mit starkem Käuferschutz. Mehr zu den Eigenheiten von Marktplätzen wie Amazon und eBay finden Sie unter [3].



Mit dem Fakeshop-Finder der Verbraucherzentralen überprüft man Shop-Websites. Bei einer roten Ampel handelt es sich nahezu sicher um einen Fake-Shop.

Hilfreich bei der Recherche ist außerdem der Fakeshop-Finder der Verbraucherzentralen. Dort gibt man die URL des zu prüfenden Online-Shops in eine Eingabemaske ein. Anschließend ordnet das Tool ihn nach einem Ampelsystem einer Kategorie zu. Zeigt die Ampel Rot, so ist der betreffende Shop bereits als Fake-Shop aufgefallen. Bei gelber Ampelfarbe hat die automatische Prüfung allgemeine Indizien für betrügerische Absichten, aber auch Indizien für seriöses Gebaren gefunden und listet sie samt Erklärung auf. Entdeckt die Prüfroutine beispielsweise kein Impressum, kann das auch heißen, dass der Betreiber des Shops es lediglich für automatisierte Abfragen gesperrt hat. Das muss man dann selbst nachsehen. Die Einstufung „Grün“ bedeutet, dass der Shop den

Verbraucherzentralen „bisher nicht negativ aufgefallen“ ist; man soll aber trotzdem auf eine sichere Zahlungsmethode und die Rücksendekonditionen achten.

Schäden begrenzen,Shops melden

Ist das Kind bereits in den Brunnen gefallen, kann man versuchen, das im Fake-Shop ausgegebene Geld zurückzubekommen. Im besten Fall hat man eine sichere Zahlungsmethode verwendet und veranlasst über seine Bank oder den Zahlungsdienstleister eine Rückerstattung. Bei einer Banküberweisung wird es hingegen schwierig. Meldet man sich sofort oder zumindest am selben Tag bei seiner Bank, kann diese die Überweisung manchmal noch stoppen.

In jedem Fall sollte man Strafanzeige bei der Polizei oder Staatsanwaltschaft erstatten. Dies geht heutzutage unkompliziert über die „Onlinewache“ (ct.de/yu3d). Zusätzlich kann man einen Rechtsanwalt damit beauftragen, den Rückzahlungsanspruch auf zivilrechtlicher Ebene durchzusetzen. Der Anwalt beantragt Einsicht in die Ermittlungsakte der Strafverfolgungsbehörden und findet im besten Fall die Identität des Betrügers heraus.

Wer einen Fake-Shop erkannt hat oder darauf hereingefallen ist, kann dazu beitragen, dass der Shop aus dem Internet verschwindet. Hat man als Betroffener Strafanzeige erstattet, kümmern sich meist Polizei und Staatsanwaltschaft darum, dass der Hoster den Shop abschaltet. Ansonsten meldet man den Fake-Shop dem Hoster oder Shopsystemanbieter sowie den Verbraucherzentralen, zum Beispiel über das Onlineformular der Verbraucherzentrale Hamburg (ct.de/yu3d). *(mon@ct.de)*

1. Literatur
2. Jo Bager, Gefährliche Offenheit, Online-Handelsregister lädt zum Datenmissbrauch ein, c’t 24/2022, S. 134
3. Markus Montz, Geld her!, Onlinekauf-Checkliste

Bezahlmethoden, c’t 8/2022, S. 26

4. Georg Schnurer, Händler-Roulette, Onlinekauf-Checkliste Shop-Auswahl, c’t 8/2022, S. 24

Nützliche Websites: ct.de/yu3d

Wie Sie sich selbst vor Phishing schützen: Empfehlungen von LeaderTelecom

Jeder kann Opfer von Internetbetrug werden. Sei es bei der Nutzung des Onlinebankings, bei Direktzahlungen über das Internet oder beim Online-Shopping mit Kreditkarte – schützen Sie sich mit diesen einfachen Tipps vor Internetbetrug.

Phishing: So fallen Sie nicht darauf herein

Eine Art des Internetbetrugs ist das Phishing. Dabei erspähen Hacker vertrauliche Daten, wie zum Beispiel Nutzernamen und Passwörter, oder Adressen und Kreditkartennummern. Sie gelangen normalerweise an diese Daten, indem Sie gefälschte Internetseiten erstellen, die dem Original sehr ähnlich sehen. Indem die Nutzer dann ihre echten Daten in die gefälschten Seiten eingeben, übermitteln sie den Betrügern unbewusst sämtliche persönlichen Informationen.

Kürzlich berichtete uns ein Nutzer des Bezahldienstes Paypal, wie er Opfer eines solchen Betrugs wurde. Roman wollte

eigentlich Geld aus seinen Devisen an sich überweisen, gelangte jedoch auf eine täuschen echte Phishing-Seite im Paypal-Stil. Er verlor dadurch 100.000 Rubel (ca. 1.400 Euro), die ihm von den Betrügern während des Vorgangs gestohlen wurden. Roman erinnerte sich später daran, dass er für die Überweisung auf die Zwei-Faktor-Verifizierung via SMS verzichtet hatte, einen Unterschied zur Original-Website hatte er in dem Moment nicht feststellen können. Grade weil es so schnell geht, sollten Sie Ihre Daten mit allen erdenklichen Mitteln schützen.

Viele Phishing-Seiten sind kaum bis gar nicht von der Original-Website zu unterscheiden. Besonders beim Surfen mit dem Handy wird die Erkennung noch schwieriger. Wie also soll man die Original-Website erkennen, und wissen, dass man ihr vertrauen kann?

Den ersten Unterschied zu einer Phishing-Seite erkennen Sie in der URL, also der Adresse in der Zeile oben im Browser. Es wird dabei von den Hackern versucht, eine ähnliche Adresse zum Original zu finden. Teilweise sind die Websites nur für wenigen Tage aktiv. Statt https://paypal.com/ steht in der Adresszeile zum Beispiel:

·t.paypal.com

·paypal-visa.com

·paypai.co

·paypal.hk

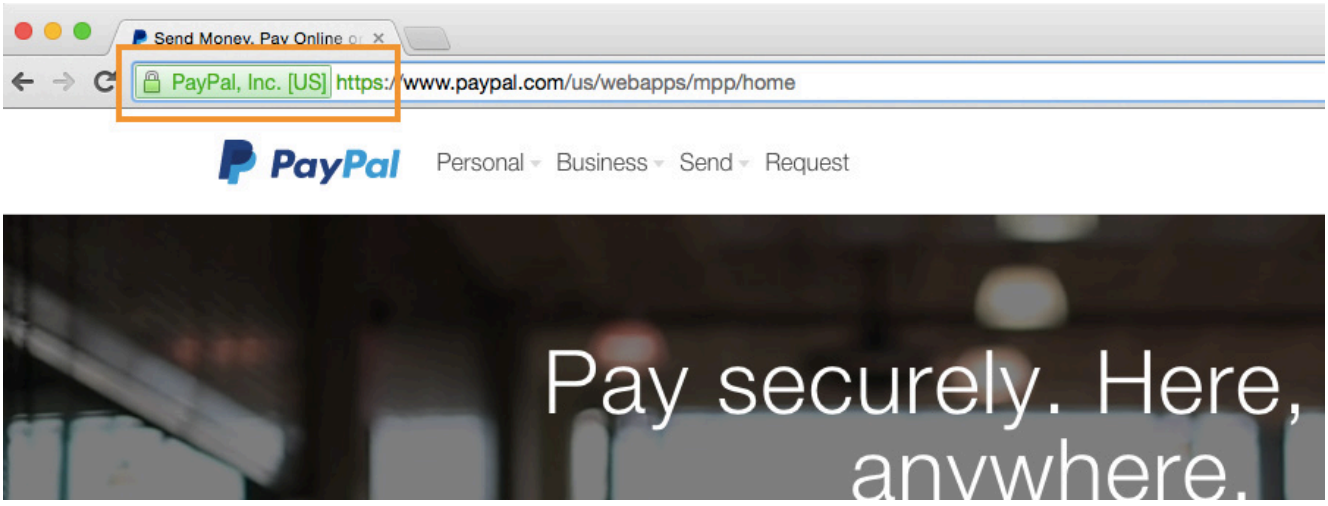
·paypl.co

Wie gelangen Internetnutzer auf diese Websites? Vor allem bei der Suche in Suchmaschinen werden die Top-Platzierungen mit Werbemitteln gekauft. Diese bezahlten Links müssen nicht zwingend etwas mit dem eigentlich gesuchten Service zu tun haben, und werden deshalb auch von Hackern genutzt. Weil der

Name jedoch ähnlich ist, übersehen einige Nutzer die fehlerhafte URL.

Der zweite Unterschied zu einer Phishing-Seite ist das fehlende SSL-Zertifikat. Heutzutage arbeiten alle Websites, auf denen Sie vertrauliche Daten eingeben können, mit einem HTTPS Protokoll zur sicheren Datenübertragung. Die allermeisten Phishing Websites nutzen hingegen noch das unsichere http-Protokoll. Solchen Seiten können Sie im Hinblick auf eine sichere Datenübertragung grundsätzlich nicht vertrauen.

Auf einer sicheren Website sehen Sie ein Schloss-Symbol in der linken Ecke der Adresszeile des Browsers. Wenn Sie auf dieses Symbol klicken, erhalten Sie weitere Details über das Zertifikat.

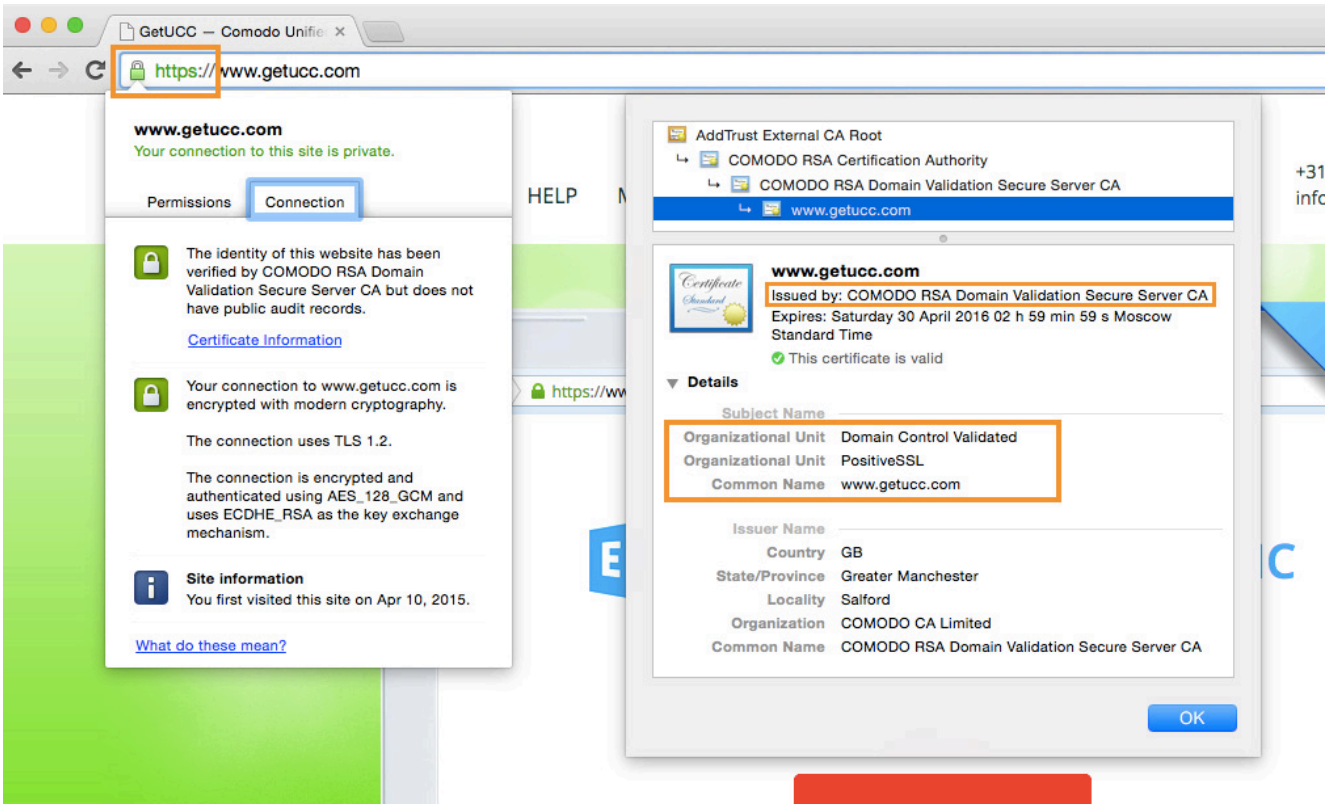


Leider nutzen zurzeit auch erste Phishing-Seiten eine gesicherte Datenübertragung und das Schloss-Symbol. In diesem Fall gilt es, ein besonderes Augenmerk auf die Art des Zertifikats zu legen: ein DV-Zertifikat schütz zwar die Daten bei der Übertragung, trifft aber keine Aussage über die Echtheit des Unternehmens selbst (z.B. Paypal).

Ein EV-Zertifikat hingegen garantiert nicht nur den sicheren Datenaustausch, es zeigt neben dem Schloss-Symbol auch den Namen des Unternehmens, welches zuvor geprüft wurde. Damit sind EV-Zertifikate die aktuell sichersten und

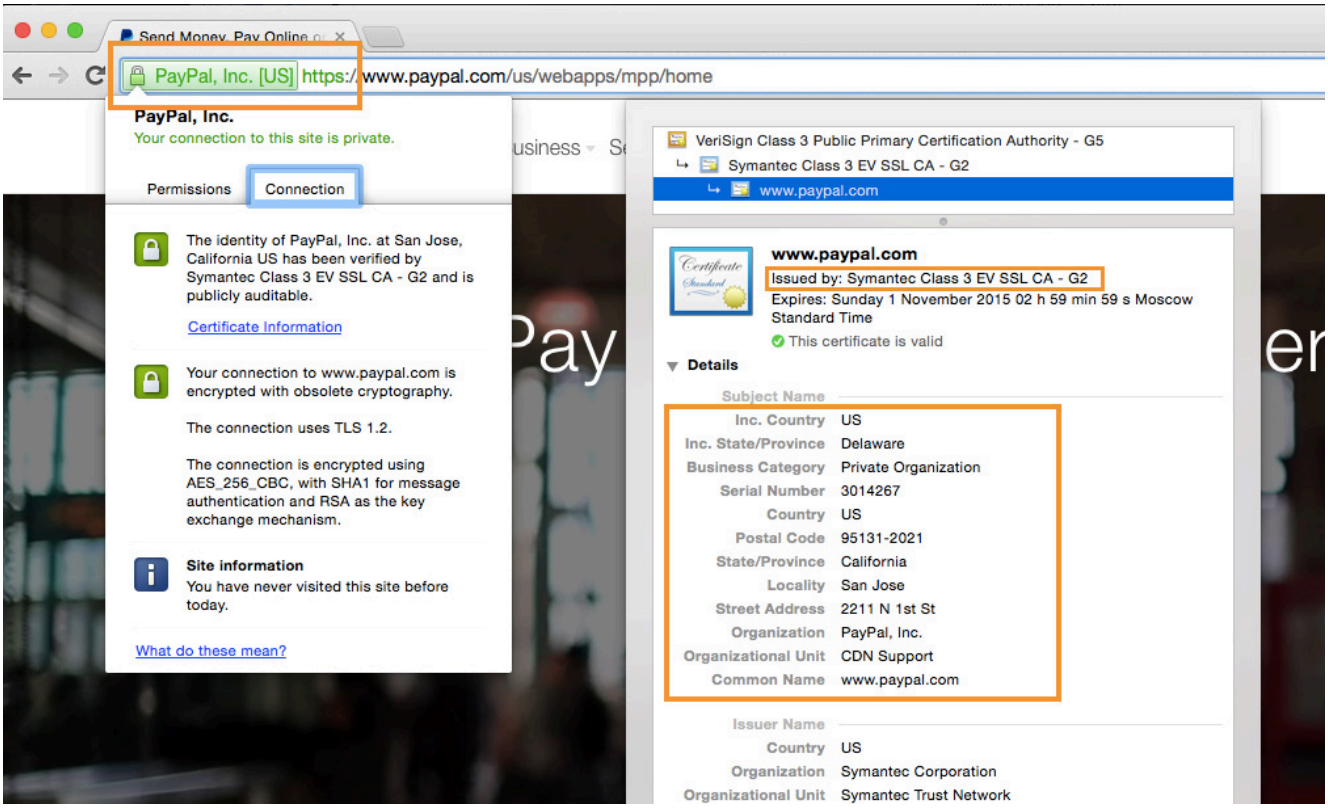
vertrauenswürdigsten Zertifikate.

Zudem färbt das Zertifikat einen Teil der Adresszeile grün und signalisiert damit jedem Nutzer die garantierte Sicherheit dieser Seite.



SSL-Zertifikat: Zum Schutz für Unternehmen

Jedes Unternehmen, welches im Internetdienste anbietet und dabei sensible Nutzerdaten verarbeitet, sollte zum größtmöglichen Schutz der Kunden ein EV SSL-Zertifikat einsetzen.



Durch den Einsatz dieses Zertifikats werden alle Informationen verschlüsselt übertragen, indem sie vor der Übermittlung in eine Buchstaben/Zahlen-Kombination umgewandelt werden. Ein Hacker könnte mit diesem Code nichts anfangen.

Unternehmen mit einem EV-Zertifikat berichten, dass sie ihren Verkauf im Bereich eCommerce zwischen 10-40% steigern konnten – das bestätigen auch unabhängige Analysten. Kaufen Sie Ihr EV-Zertifikat gleich hier.

Was ist SSL?

Was ist SSL?

SSL ist ein Akronym für Secure Sockets Layer. SSL bietet eine sichere Verbindung, mit der Sie private Daten online

übertragen können. Mit SSL gesicherte Websites zeigen ein Vorhängeschloss in der Browser-URL und möglicherweise eine grüne Adressleiste an, wenn sie durch ein EV-SSL-Zertifikat gesichert sind.

Das SSL-Protokoll wird von Millionen von E-Business-Anbietern verwendet, um ihre Kunden zu schützen und sicherzustellen, dass ihre Online-Transaktionen vertraulich bleiben. Um das SSL-Protokoll nutzen zu können, benötigt ein Webserver die Verwendung eines SSL-Zertifikats.

Websites erhalten eine SSL-Verschlüsselung, um alle Bereiche abzudecken, die einen Datenaustausch beinhalten, einschließlich Login-Boxen, Kreditkartenzahlungen oder persönliche Informationen. Alle Webbrowser können mit SSL-gesicherten Websites interagieren, solange das SSL der Websites von einer anerkannten Zertifizierungsstelle wie Comodo stammt.

Warum benötige ich SSL auf meiner Website

Das Internet hat erfolgreich viele neue globale Geschäftsmöglichkeiten für Unternehmen geschaffen, die Online-Handel betreiben. Dieses Wachstum hat jedoch auch Betrüger und Cyberkriminelle angezogen.

Das zunehmende Bewusstsein für Online-Betrüger und Cyberkriminelle bietet E-Commerce-Anbietern die Möglichkeit, die Ängste der Verbraucher zu nutzen, indem sie Vertrauensindikatoren anzeigen. Genau wie in der realen Welt müssen Menschen zuversichtlich sein, bevor sie einen unbekannten Weg einschlagen.

Wie funktioniert SSL?

Wenn ein digitales SSL-Zertifikat auf einer Website installiert ist, sehen Benutzer ein Vorhängeschloss-Symbol im unteren Bereich des Navigators. Wenn ein Extended Validation Certificate auf einer Website installiert ist, sehen Benutzer mit den neuesten Versionen von Firefox, Internet Explorer oder Opera die grüne Adressleiste im URL-Bereich des Navigators.

Benutzern auf Websites mit SSL-Zertifikaten wird während einer E-Commerce-Transaktion auch https:// in der Adressleiste angezeigt.

Wildcard EV-Zertifikate: welche Möglichkeiten gibt es?

Ein EV-Zertifikat ist eine großartige Möglichkeit, Ihre Website vor dem Diebstahl von Benutzerdaten zu schützen. Viele Online-Shops verwenden diese Zertifikate, um das Vertrauen ihrer Kunden in ihre Website noch zu erhöhen. Letztendlich erhalten Sie durch diese Zertifikate für Ihre Website im Browser eine grüne Adresszeile, was Nutzer auf die höchste Sicherheitsstufe beim Browsen hinweist.

Heutzutage wären Website-Betreiber dazu bereit, ein Wildcard EV-Zertifikat zu kaufen, welches eine unbegrenzte Anzahl von Subdomains mit dem grünen Sicherheitssymbol im Browser schützt. Aber solch ein SSL-Zertifikat existiert gar nicht. Hier erfahren Sie die Gründe, und welche Alternativen es gibt.

Warum gibt es keine Wildcard EV-Zertifikate?

EV-Zertifikate bieten die höchste Stufe an Vertrauenswürdigkeit unter allen Arten von SSL-Zertifikaten. Um eine unsachgemäße Anwendung von EV-SSL-Zertifikaten zu vermeiden, verlangt die SSL-Regulierungsbehörde, die für das Aufstellen der Regeln zur Erteilung von SSL-Zertifikaten verantwortlich ist (bekannt als das CA/B Forum), die Überprüfung jedes einzelnen Hosts, der mit einem Zertifikat verbunden ist. Aus diesem Grund ist der Kauf eines Wildcard EV-Zertifikats für unbegrenzte Subdomains nicht möglich. Ein "Wildcard" Zertifikate schützt per Definition eine unbegrenzte Anzahl von Subdomains, die durch ein Sternchen eingebunden sind (z.B. * .domain.com) und nicht explizit aufgelistet werden müssen.

Wenn Sie Ihre Subdomains durch die Anwendung des EV-Zertifikats schützen wollen, können Sie in der Praxis Folgendes tun:

1. Kaufen Sie mehrere separate EV-SSL-Zertifikate.

Diese Möglichkeit ist ideal, wenn Sie nur eine geringe Anzahl von Subdomains haben, die Sie schützen wollen. In diesem Fall können Sie für jede Subdomain ein einzelnes EV-Zertifikat ausstellen. Der Nachteil dieser Option ist, dass Sie wahrscheinlich (abhängig davon, wo Sie den Auftrag erteilen) die notwendigen Daten für jedes einzelne Zertifikat separat eingeben müssen. Das ist für den Nutzer etwas unpraktisch. Solche EV-Zertifikate können SIe auf der LeaderTelecom Website bestellen.

2. Kaufen Sie ein EV Multi-Domain Zertifikat.

Diese Option ist günstiger, weil das Multi-Domain-Zertifikat eine ausreichend große Anzahl von Domains (einschließlich Subdomains) abdeckt. Der Kauf dieses Zertifikats ist sehr

rentabel, wenn Sie viele Domains / Subdomains haben, die Sie damit schützen wollen. Je mehr Domainnamen Sie hinzufügen, umso effizienter wird das Multi-Domain-Zertifikat im Vergleich zum Standard EV-Zertifikat. Außerdem braucht der Nutzer nur einen Antrag für ein Zertifikat stellen, in dem alle Domainnamen enthalten sind. Damit kann er viel Zeit sparen.

Zusätzliche Domainnamen können dem Zertifikat hinzugefügt werden, auch nachdem es bereits ausgestellt wurde. Das ist dann besonders günstig, wenn einer Ihrer Domainnamen noch nicht bekannt ist. Auch das EV-Multi-Domain-Zertifikat können Sie auf der LeaderTelecom Website bestellen.

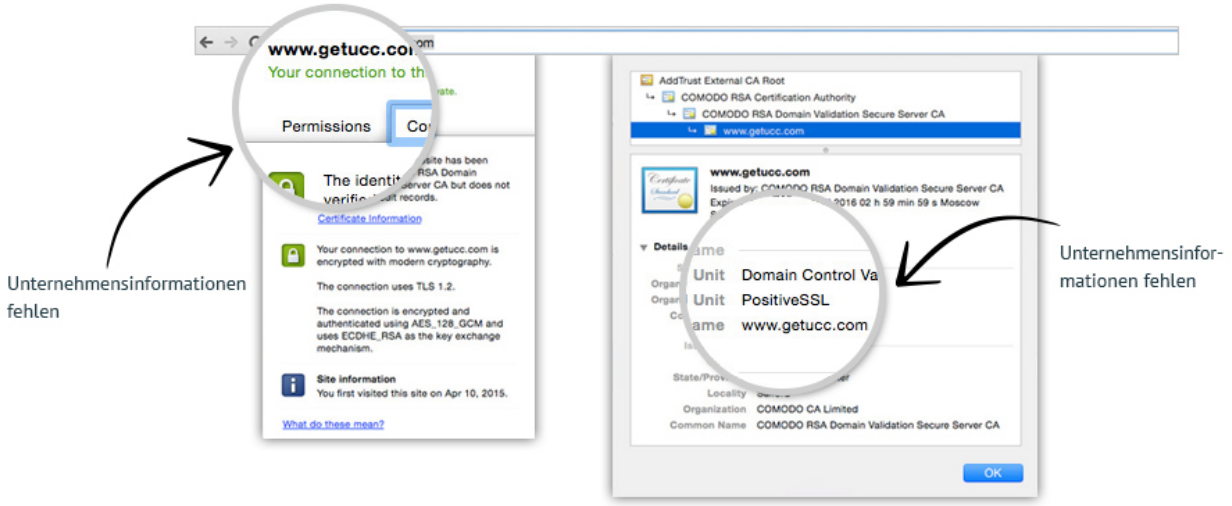
Ein weiterer Vorteil des Multi-Domain-Zertifikats gegenüber separaten EV-Zertifikaten ist die einfache Verwaltung. Es ist viel einfacher, ein einzelnes Multi-Domain-Zertifikat zu verwalten als mehrere einzelne Zertifikate. Außerdem können Sie durch Multi-Domain-Zertifikate Geld sparen (mehr Websites, mehr Ersparnis). Aus diesen Gründen kaufen bereits immer mehr Betreiber mehrerer Websites ein Multi-Domain-EV-Zertifikat. Ein solches EV-Multi-Domain-Zertifikat können Sie jederzeit auf der LeaderTelecom Website mit einem guten Rabatt kaufen.

Unterschied zwischen DV- und OV-Zertifikaten

Wir wissen bereits, dass man SSL-Zertifikate in drei Typen unterteilt: DV, OV und EV. In diesem Artikel erklären wir die ersten beiden Zertifikate, DV und OV. Erfahren Sie im Folgenden mehr über ihre Unterschiede und Einsatzmöglichkeiten, und wann Sie welches Zertifikat benötigen.

Bei einem DV-Zertifikat steht die Abkürzung für Domain Validation, das bedeutet eine Validierung/Überprüfung der Domain. Dies ist das grundlegende Level für ein SSL-Zertifikat. Eine Zertifizierungsstelle (Certification Authority (CA)) bestätigt damit, dass Sie der Inhaber einer bestimmten Domain sind, und damit die Informationen des WHOIS-Eintrags. Dieses Zertifikat erlaubt selbstverständlich wie gewünscht eine sichere Datenverschlüsselung auf Ihrer Website, aber es verifiziert Sie nicht als Besitzer eines rechtmäßigen Unternehmens. Trotzdem ist dies ein absolut zulässiges Zertifikat und eine sehr schnelle Lösung für den effektiven Schutz einer Website per HTTPS. Dank des weit bekannten Schloss-Symbols neben der Adressleiste im Browser werden Kunden Ihrer Website im höheren Maße als vorher vertrauen.

Beispiel für ein DV-Zertifikat:



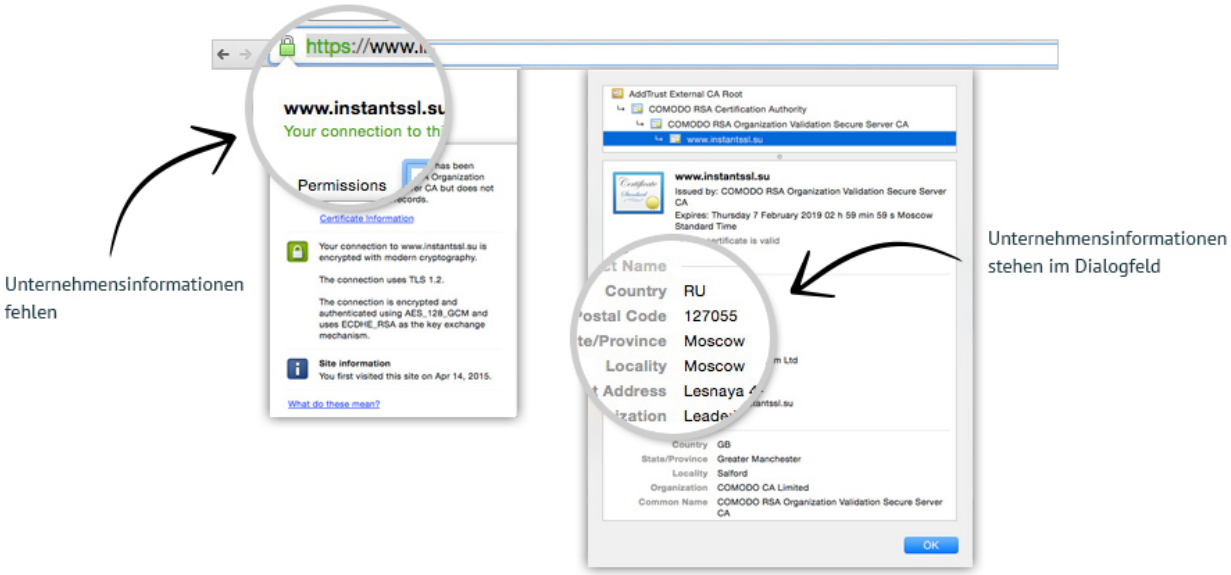
Ein DV-Zertifikat bietet sich überall da an, wo Sicherheit eine wichtige, aber keine übergeordnete Rolle spielt. Denn auch Internetbetrügern und Hackern ist es leider möglich, DV-Zertifikate für Ihre gefälschten Phishing-Seiten zu verwenden. Hier werden arglose Nutzer mittels des vermeintlich sicheren Schloss-Symbols dazu verleitet, ihre persönlichen Daten anzugeben, welche dann in die Hände der Kriminellen fallen. Nur weil die Datenübertragung verschlüsselt wird heißt das nämlich nicht, dass die Daten auch beim richtigen Empfänger

ankommen. Internetnutzer müssen deshalb auch sichergehen können, dass die aufgerufene Website auch zu einem rechtmäßigem Unternehmen gehört, bevor sie einen Kauf abschließen oder private Daten angeben.

Aus diesem Grund empfehlen wir für Websites mit höchsten Sicherheitsansprüchen ein OV-Zertifikat.

Ein OV-Zertifikat als Abkürzung für Organisation Validation, also mit einer Überprüfung des Unternehmens, benötigen vor allem Firmen und Organisationen, bei denen Kunden sensible Daten (Kreditkartennummern, Kontaktdaten, etc.) angeben müssen. Sie eignen sich damit insbesondere für eCommerce-Seiten und jede Art von Onlineverkauf. Ein OV-Zertifikat beglaubigt die Echtheit des Inhabers einer Website und benötigt dafür rechtmäßige Unternehmensinformationen von einer Firma. Der Validierungsprozess für solche Zertifikate dauert deshalb etwas länger und ist umfangreicher. Die Zertifizierungsstelle bescheinigt nicht nur, dass Ihnen die entsprechende Domain gehört, sondern auch, dass Sie der rechtmäßige Besitzer des Unternehmens sind. Dafür muss die Firma in einem Unternehmensregister und einem Onlineverzeichnis gelistet sein, zum Beispiel dnd.com. Kriminelle können kein solches OV-Zertifikat bekommen, weil sie ihre „Firma“ nicht rechtmäßig überprüfen lassen können. Der Hauptvorteil eines OV-Zertifikats liegt darin, dass Ihr Unternehmen auf dem Zertifikat namentlich genannt wird.

Beispiel für ein OV-Zertifikat:



Erwägen Sie den Wechsel von einem DV-Zertifikat auf ein OV-Zertifikat, wenn:

- Sie sensible Nutzerdaten schützen müssen
- der Name Ihres Unternehmens auf dem Zertifikat stehen soll (für ein höheres Vertrauen der Nutzer)
- Sie Ihre Geschäftstätigkeiten ausweiten und auf ein neues Level heben möchten
- Nutzer Ihre Website als rechtmäßiges Unternehmen und keinesfalls als Phishing-Seite wahrnehmen sollen

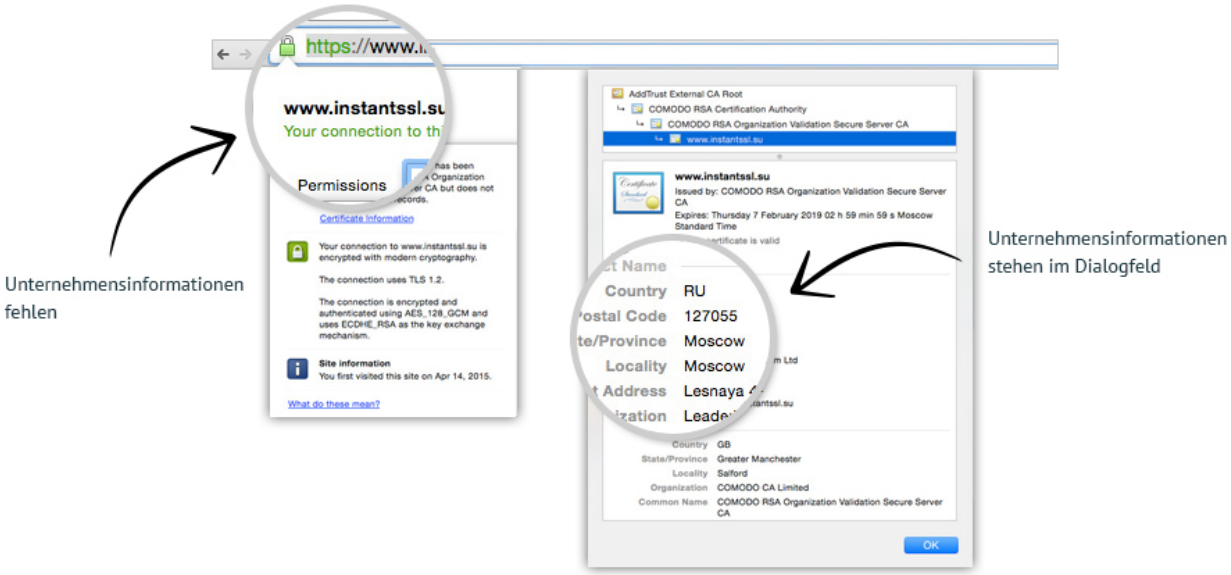
Wenn Sie noch Fragen zu einem Zertifikatswechsel haben, oder überlegen von einem DV- auf ein OV-Zertifikat umzusteigen, fragen Sie unsere Experten von LeaderTelecom. Mit unserer jahrelangen Erfahrung und schlanken Prozessen bei der Kommunikation mit den Zertifizierungsstellen stellen wir Ihnen jede Art von Zertifikat komfortabel und schnell aus.

Unterschied zwischen OV- und EV-Zertifikaten

SSL-Zertifikate sind heutzutage eine wesentliche Voraussetzung für eCommerce-Seiten. Schwer vorstellbar, dass eine glaubwürdige Unternehmensseite nicht sicher sein könnte. Jeder Zweifel würde einen Kunden davon abhalten, auf einer solchen Seite einen Onlinekauf zu tätigen. Aus diesem Grund sollten Sie als Inhaber eines rechtmäßigen Unternehmens mit einem Online-Shop auf jeden Fall über den Einsatz eines SSL-Zertifikats nachdenken. Dabei stellt sich vielen Domain-Inhabern die Frage: Welcher Zertifikatstyp ist der richtige, OV oder EV? Und wo liegt der Unterschiede zwischen diesen beiden SSL-Zertifikaten?

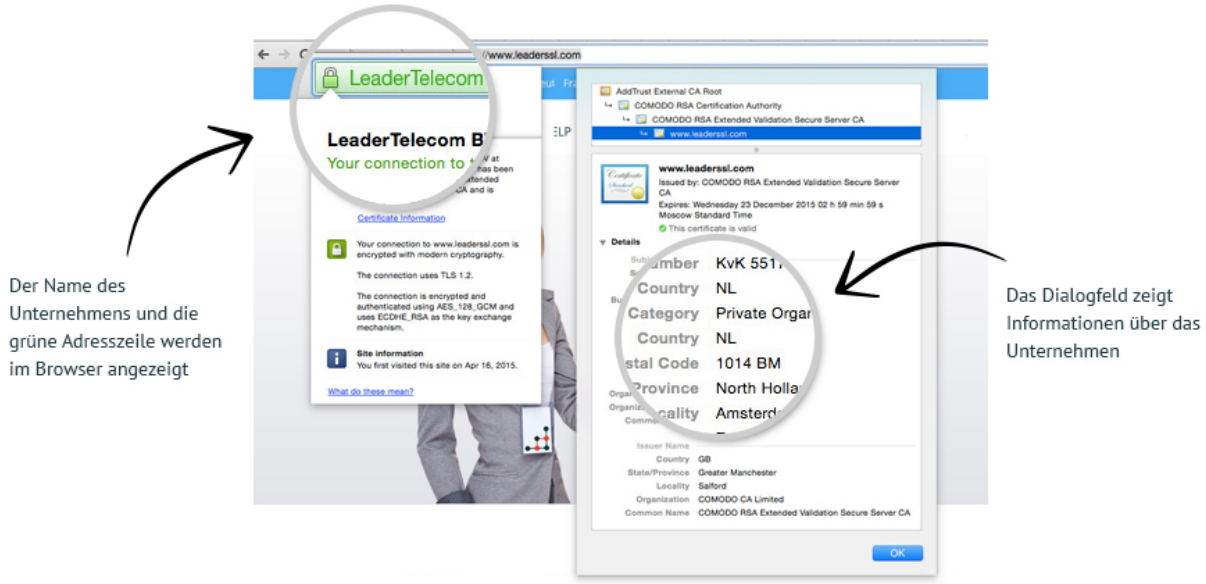
Ein OV-Zertifikat mit der Abkürzung OV für Organisation Validation, was sich mit Unternehmensüberprüfung übersetzen lässt, verifiziert die Echtheit einer Organisation oder einer Firma. Für das Ausstellen eines OV-Zertifikats muss ein Unternehmen zunächst den Validierungsprozess abschließen. Darin bestätigt die Zertifizierungsstelle die Existenz des Unternehmens mittels eines Abgleichs mit einem staatlicher Unternehmensregister und einem Onlineverzeichnis. Sobald die gewünschte Website per OV-Zertifikat gesichert ist, sehen die Internetnutzer das bekannte Schloss-Symbol neben der Adressleiste im Browsers und wissen damit um den Schutz der Seite vor Hackern.

Beispiel für ein OV-Zertifikat:



EV-Zertifikate, welche für Extended Validation, also eine erweiterte Überprüfung stehen, gelten derzeit als sicherste und vertrauenswürdigste Lösung für die weltweit führenden Online-Unternehmen. Das Zertifikat beinhaltet das Anzeigen einer grünen Browser-Adresszeile als Zeichen für Sicherheit und Zuverlässigkeit. Außerdem wird auch der Name des Unternehmens bei einem EV-Zertifikat direkt im Browserfenster mit angezeigt, wie Sie auf dem Screenshot unten sehen können. Damit erfassen Internetnutzer schnell, dass diese Website von einer rechtmäßigen Firma und nicht von Hackern betrieben wird. Das Ausstellen eines EV-Zertifikats ist nicht viel aufwendiger, als das Vorgehen bei einem OV-Zertifikat – trotzdem bietet es eine höhere Stufe an Sicherheit und Vertrauen. Dank des Zertifikats fühlen sich Internetnutzer beim Surfen aus Ihrer Website sicherer, und das gesteigerte Vertrauen wird Ihre Verkaufszahlen ankurbeln.

Beispiel für ein EV-Zertifikat:



- EV-Zertifikate beinhalten ein grafisches Symbol (die grüne Adresszeile im Browser), als bewährtes Zeichen für Glaubwürdigkeit selbst für unerfahrene Internetnutzer
- EV-Zertifikate zeigen den Namen des Unternehmens (direkt in der Adresszeile des Browsers) und weiterführende Informationen darüber an
- EV-Zertifikate sind nicht viel teurer als OV-Zertifikate, haben aber mehr Vorteile
- EV-Zertifikate werden von weltweit tätigen Unternehmen bevorzugt

Falls Sie den Wechsel zu einem EV-Zertifikat in Betracht ziehen, sich aber noch vor dem Validierungsprozess scheuen, sprechen Sie uns gerne an! Gerne übernehmen unsere Experten von LeaderTelecom diese Aufgabe für Sie. Mit unserer jahrelangen Erfahrung und vielfach bewährten Prozessen helfen wir Ihnen in kürzester Zeit zu einem eigenen EV-Zertifiakt.

Social-Engineering-Angriffe auf Instagram-Accounts und wie Sie sich davor schützen

Instahack

Social-Engineering-Angriffe auf Instagram-Accounts und wie Sie sich davor schützen

Immer wieder kapern Phisher fremde Instagram-Accounts, um Profit daraus zu schlagen. So auch im Fall einer deutschen Olympiaschwimmerin, die sich Hilfe suchend an c’t wandte. Wir sind der Sache nachgegangen und stießen dabei auf weitere Fälle. Wir erklären, wie Sie Ihren Account schützen.

Von Ronald Eikenberg und Marie-Claire Koch

kompakt

- Instagram-Accounts, egal ob sehr populär oder nahezu unbekannt, sind ein lukratives Angriffsziel für Cyber-Kriminelle.
- Es ist wichtig, den Account mehrstufig abzusichern, wenn man nicht Gefahr laufen will, ihn für immer zu verlieren.
- Wer eine Mail erhält, die angeblich von Instagram stammt, sollte in der App kontrollieren, ob die Mail echt ist.

Phisher versuchen immer wieder an Zugangsdaten für Social-Media-Dienste wie Instagram zu kommen, um Accounts zu kapern

und Profit daraus zu schlagen [1] – zum Beispiel durch Lösegeldforderungen oder dubiose Spam-Kampagnen. Dafür ist den Angreifern jeder Account gut genug, doch besonders hoch im Kurs stehen Instagram-Accounts, die der begehrte blaue Haken ziert. Er zeigt, dass es sich um ein durch Instagram verifiziertes Profil einer Person öffentlichen Interesses handelt. Aber auch mit nicht verifizierten Accounts können Phisher Geld machen, mangelndes öffentliches Interesse schützt Ihren Account daher nicht.

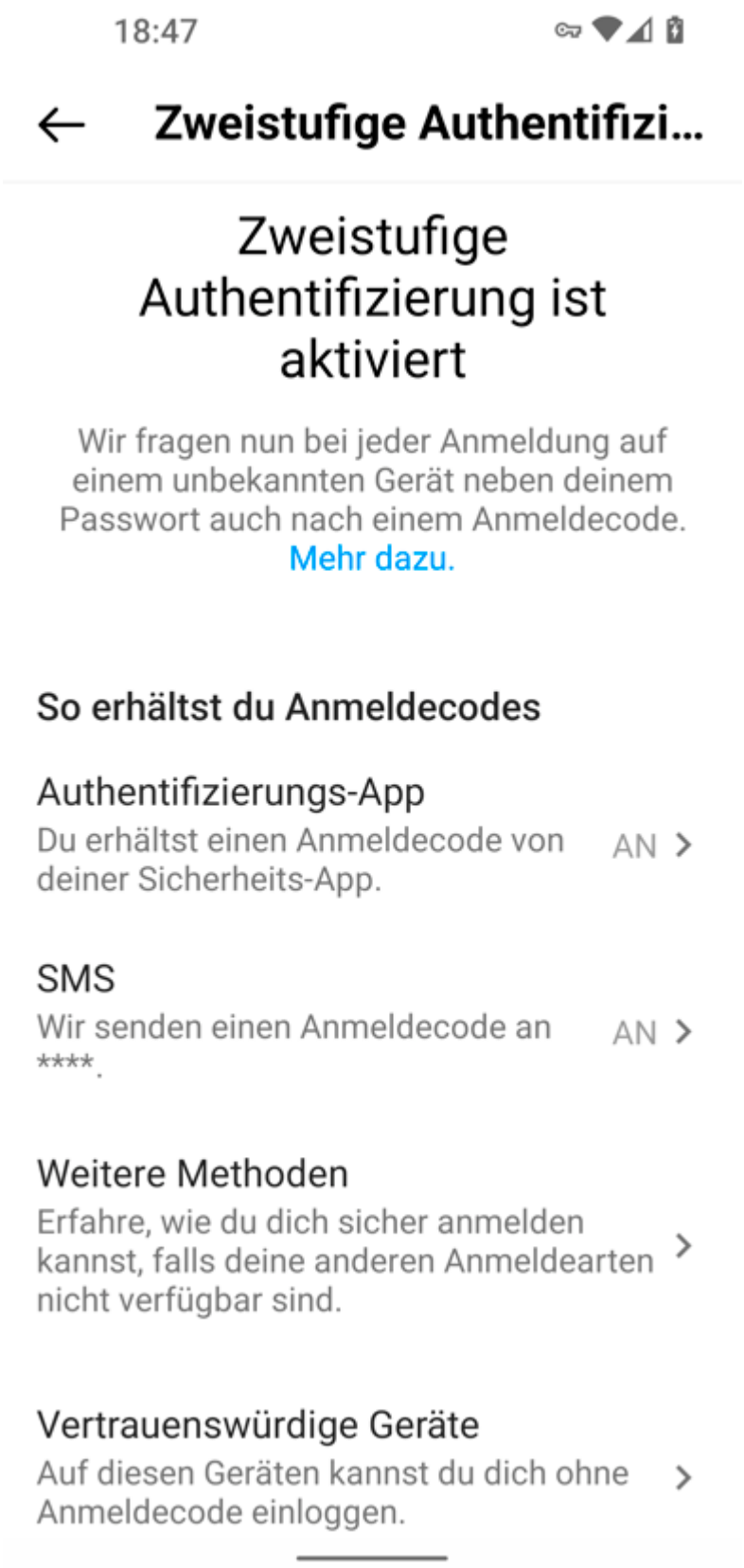
Der Instagram-Account einer Berliner Olympiaschwimmerin trägt diesen blauen Haken. Sie nutzt den Account, um mit ihren Fans in Kontakt zu bleiben und ihre Erfolge zu teilen – zum Beispiel ihre Teilnahme an den Olympischen Spielen in Tokio oder zuletzt an der Europameisterschaft in Rom. Vor einigen Monaten entdeckte auch ein Phisher die erfolgreiche Schwimmerin bei Instagram. Er kontaktierte sie über eine private Nachricht, gab sich als Instagram-Support aus, um sie in die Falle zu locken, und konnte letztlich die Kontrolle über ihren Account übernehmen.

Man spricht bei solchen Angriffen von Social Engineering, also der gezielten Manipulation des Opfers. Als die Schwimmerin bemerkte, wie ihr geschah, war das Kind bereits in den Brunnen gefallen. Der Angreifer hatte das Instagram-Konto bereits fest im Griff und die Account-Sprache auf Arabisch geändert. Die Schwimmerin wandte sich daraufhin an einen IT-Experten, der den Account jedoch auch nicht mehr retten konnte. Der Täter forderte unterdessen ein Lösegeld in Höhe von 150 Euro, zahlbar via PayPal.

Passwort: „Passwort“

Statt der dreisten Lösegeldforderung nachzukommen, wandten sich die beiden an c’t. Im Rahmen unserer Recherche stießen wir auf drei weitere Sportlerinnen und Sportler aus dem Umfeld der Schwimmerin, deren Accounts ebenfalls gehackt waren. In zwei Fällen war ebenfalls Social Engineering im Spiel, im

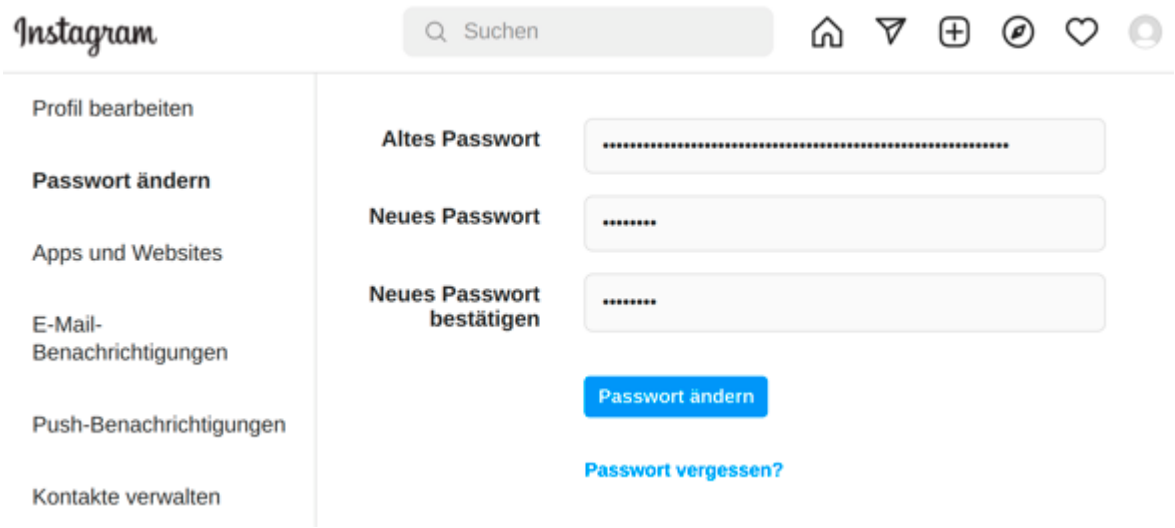
dritten wurde offenbar das Passwort erraten – es lautete schlicht „Passwort“. Alle betroffenen Accounts waren nicht nach Stand der Technik abgesichert: Die sogenannte Zwei-Faktor-Authentifizierung (2FA), die Angriffe auf Online-Accounts in den meisten Fällen vereiteln kann [2], war nicht eingeschaltet.



Wer einen Instagram-Account besitzt, sollte die zweistufige Authentifizierung einschalten.
Ist die 2FA aktiv, ist zumindest beim ersten Einloggen auf einem Gerät neben dem Passwort auch noch ein zweiter Faktor nötig. Das kann zum Beispiel ein kurzzeitig gültiger

Zahlencode sein, den man per SMS bekommt oder mit einer App wie dem Google Authenticator selbst generiert. Ein Hacker kommt in aller Regel nicht an SMS und erst recht nicht an das Geheimnis in der Authenticator-App. Mit einem erbeuteten Passwort kann er sich daher nicht einloggen.

Um die gehackten Instagram-Accounts der Athleten zu retten, kontaktierten wir die Pressestelle des Instagram-Betreibers Meta. Kurz darauf konnten die rechtmäßigen Account-Besitzer wieder auf ihre Konten zugreifen. Uns erreichen immer wieder ähnliche Zuschriften von Instagram-Nutzern, die Opfer von Cyber-Ganoven geworden sind. Weil wir nicht immer helfen können und damit es erst gar nicht so weit kommt, möchten wir Ihnen im Folgenden die wichtigsten Sicherheitstipps an die Hand geben, damit Sie Ihren Instagram-Account – oder die Accounts Ihrer Sprösslinge – angemessen absichern können.



Passwort: „Passwort“ – die Passwortanforderungen von Instagram sind eher locker, damit haben Cyber-Ganoven wie in diesem Fall dann leichtes Spiel.

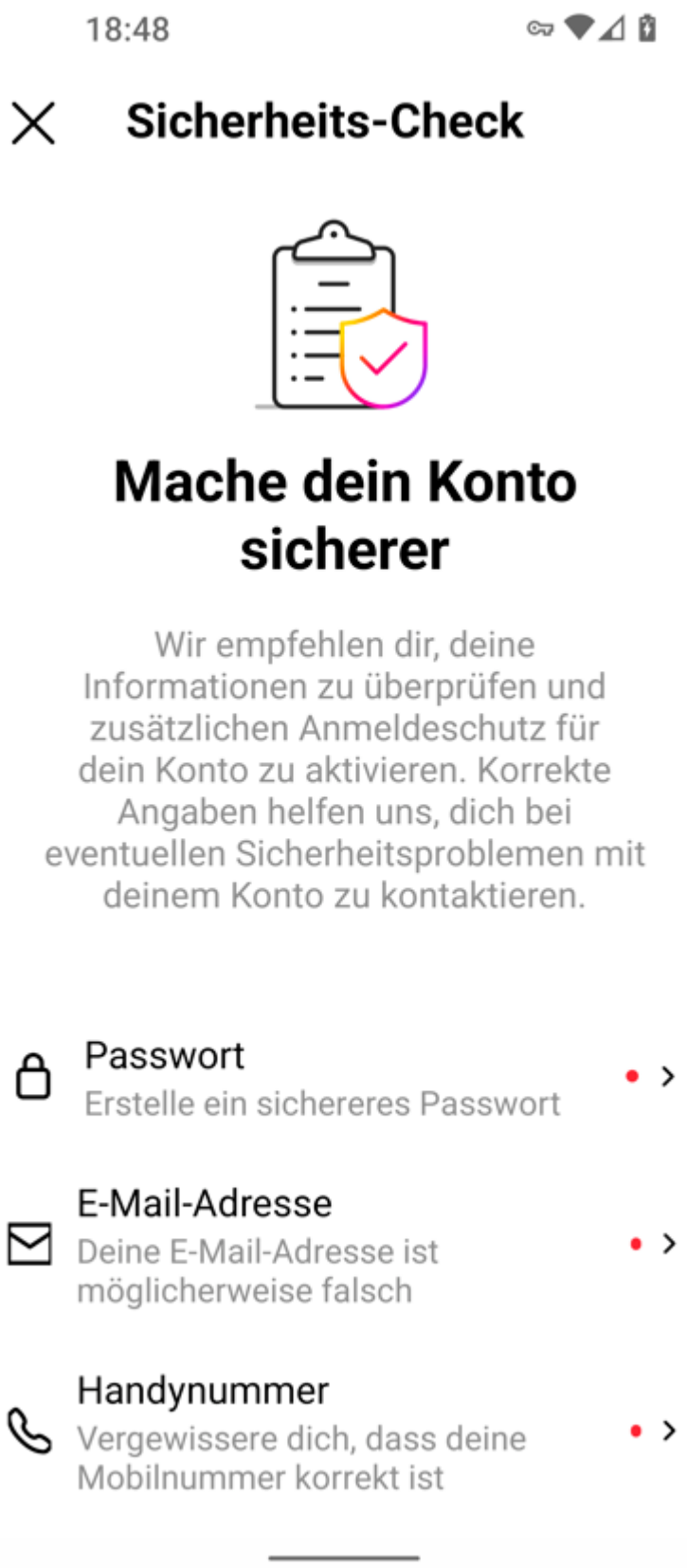
Instagram-Account absichern

Der beste Zeitpunkt, um sich um die Sicherheit Ihres Instagram-Accounts zu kümmern, ist genau jetzt, nicht später heute Abend oder am Wochenende. Sie müssen nur wenig Zeit investieren und ersparen sich früher oder später viel Ärger. Wenn Sie die von Instagram bereitgestellten Werkzeuge kennen

und nutzen, ziehen die meisten Angreifer unverrichteter Dinge zum nächsten Account weiter, der womöglich weniger gut abgesichert ist.

Den effektivsten Schutz gegen Phishing-Angriffe bietet die bereits erwähnte Zwei-Faktor-Authentifizierung (2FA), die Instagram „Zweistufige Authentifizierung“ nennt. In der Instagram-App aktivieren Sie den Schutz über den Menüknopf oben rechts und „Einstellungen/Sicherheit/Zweistufige Authentifizierung“, auf der Website klicken Sie in den Einstellungen auf „Privatsphäre und Sicherheit“, um die zweistufige Authentifizierung zu finden. Anschließend haben Sie die Wahl, ob Sie die zum Einloggen nötigen Zahlencodes per SMS zugeschickt bekommen möchten oder lieber selbst generieren wollen, mit einer Authenticator-App auf dem Smartphone.

Die SMS-Variante ist einfacher, aber auch unsicherer, weil es Angreifern gelingen kann, die SMS-Nachrichten mit den Codes abzufangen. Dennoch ist 2FA per SMS besser als nichts. Wir empfehlen die sicherere Variante „Authentifizierungs-App“, die sie jedoch nur mit der Instagram-App aktivieren können, nicht über die Website. Anschließend empfiehlt Ihnen Instagram geeignete Authenticator-Apps wie die von Google und erklärt Ihnen, wie Sie diese mit Ihrem Instagram-Account verknüpfen. Darüber hinaus sollten Sie ein langes Passwort für Ihren Account wählen, das nicht zu erraten ist und nur bei Instagram passt. Im besten Fall nutzen Sie einen Passwortmanager, um ein langes Zufallspasswort zu generieren und zu speichern.



Mit dem Sicherheits-Check überprüfen Sie die wichtigsten Security-Einstellungen bei Instagram.

Sicherheits-Check

Hilfreich ist der „Sicherheits-Check“, den Sie ebenfalls über die Sicherheitseinstellungen in der Instagram-App starten können. Diese Funktion macht auf gängige Sicherheitsprobleme wie ein schwaches Passwort aufmerksam und empfiehlt auch das Einschalten der 2FA, sofern sie nicht bereits aktiv ist. Zudem erinnert der Sicherheits-Check daran, dass man die Aktualität der hinterlegten Mailadresse und Telefonnummer kontrollieren sollte.

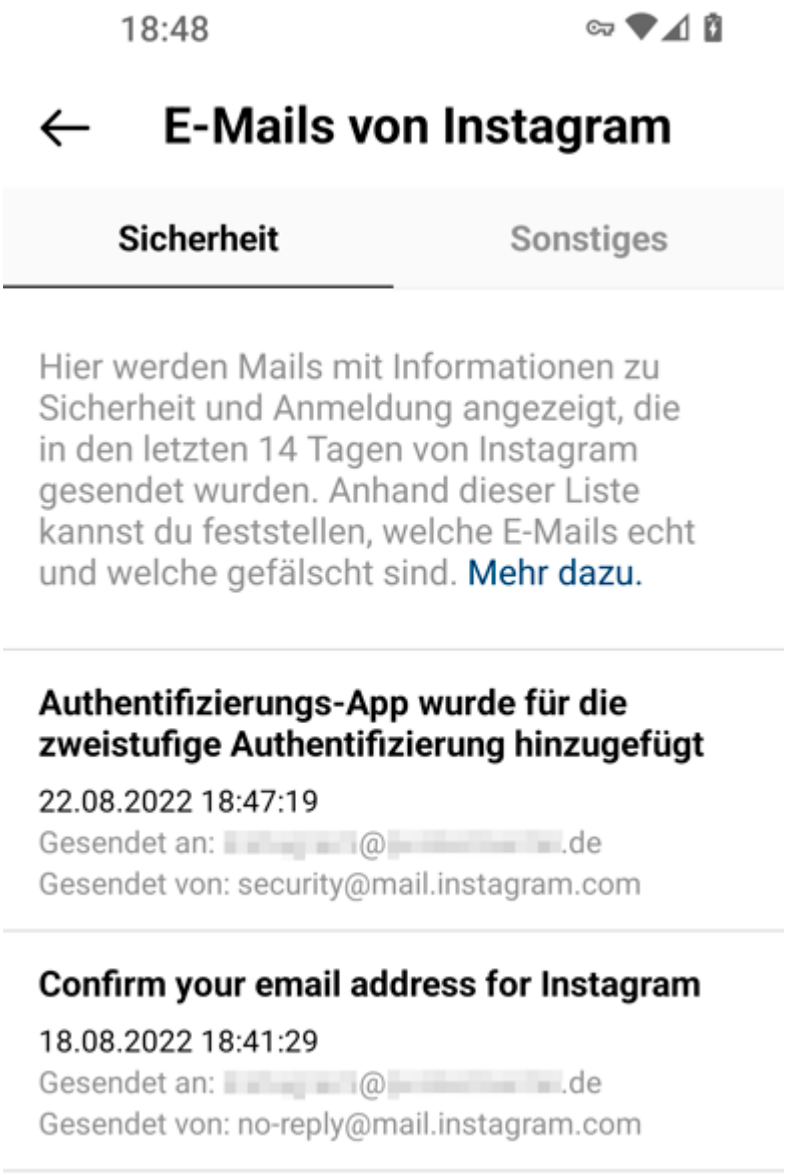
Wenn Sie Instagrams Betreiberfirma Meta diese Daten nicht anvertrauen möchten, funktionieren viele der Rettungsfunktionen von Instagram nicht, etwa weil das Unternehmen Ihnen im Fall der Fälle keinen Link zuschicken kann, über den Sie die Kontrolle über den gehackten Account zurückgewinnen können. Keine ganz leichte Abwägung, eventuell können Sie Instagram eine Zweit- oder Drittmailadresse zur Verfügung stellen – Hauptsache, Sie haben im Notfall sicher Zugriff darauf. Auch ein Profilfoto, auf dem Sie gut zu erkennen sind, kann die Rettung des Accounts erleichtern. Dazu gleich mehr.

Anti-Social-Engineering

Auch wenn Sie Ihren Account mit allen zur Verfügung stehenden Mitteln abgesichert haben: Technische Schutzmaßnahmen können Social Engineering nur erschweren, nicht verhindern. Angreifer hacken nicht Ihr Smartphone, sondern locken Sie trickreich in die Falle, etwa indem sie sich eben als Instagram-Support ausgeben und Sie mit einer plausibel klingenden Geschichte auffordern, Ihre Zugangsdaten auf einer externen Website einzugeben. Der zweite Faktor erschwert zwar einen solchen Phishing-Angriff, doch in jüngster Zeit fragen Online-Ganoven immer wieder auch nach dem temporären Einmalcode, mit dem sie den Account schließlich übernehmen können.

Allerdings können Sie sich vor dieser Form des Social

Engineering leicht schützen. Zunächst einmal sollten Sie sich darüber im Klaren sein, dass Sie Instagram niemals per Direktnachricht (Direct Message, DM) kontaktieren wird. Bei DMs ist Vorsicht geboten, auch wenn Sie den Absender kennen: Wurde ein Account gehackt, nehmen Angreifer schon mal Kontakt mit Freunden und Followern des Opfers auf, meist um die dazu zu bringen, eine gefährliche Website zu besuchen.



In der Instagram-App können Sie überprüfen, ob eine Mail, die angeblich von Instagram stammt, tatsächlich echt ist.

Mailcheck

Instagram kontaktiert Sie ausschließlich per Mail. Das wissen

allerdings auch die Cyber-Ganoven, sie verschicken täuschend echt aussehende Phishing-Mails im Instagram-Look. Wenn Sie eine Mail bekommen, die von Instagram stammen soll, sollten Sie sich also zunächst von der Echtheit überzeugen, bevor Sie die Mail ernst nehmen und auf einen Link aus der Nachricht klicken. Das ist bei Instagram erfreulich einfach: Öffnen Sie die Einstellungen in der App und tippen Sie auf „Sicherheit/E-Mails von Instagram“.

Dort listet die App alle Nachrichten auf, die Ihnen Instagram in den vergangenen 14 Tagen per Mail geschickt hat. Sie können die Nachrichten dort zwar nicht lesen, aber Sie erfahren Absender, Betreff und Sendedatum. Gleichen Sie diese Daten mit der Mail ab, um die Echtheit der Mail zu verifizieren. Der Absender sicherheitsrelevanter Instagram-Mails lautet stets security@mail.instagram.com. Wenn Sie auf Nummer sicher gehen wollen, dass der angegebene Absender nicht gefälscht ist, können Sie den Mail-Header inspizieren, wie in ct 19/2022 beschrieben [1].

Gehackten Account retten

Ist das Kind bereits in den Brunnen gefallen und Ihr Account wurde gehackt, dann müssen Sie schnell handeln. Je früher Sie aktiv werden, desto mehr Schaden können Sie abwenden. Nutzen Sie für sämtliche Rettungsversuche am besten ein Gerät, mit dem Sie bereits zuvor bei Instagram eingeloggt waren.

Beachten Sie die Mails von Instagram, um frühzeitig von einer Account-Übernahme zu erfahren. Der Dienst wird Sie über den Fremdlogin per Mail informieren und liefert Ihnen nicht nur den Zeitpunkt des Logins, Sie erfahren auch, welches Betriebssystem und welcher Browser mutmaßlich zum Einsatz kam. Zudem führt Instagram das Land an, aus dem die IP-Adresse des Nutzers stammt.

Auch wenn diese Daten nicht zu einhundert Prozent verlässlich sind: Sie eigenen sich gut, um darin Abweichungen zu Ihren

bisherigen Anmeldungen zu erkennen. Falls Ihnen bei der Kontrolle der Loginaktivität etwas komisch vorkommt, können Sie Ihren Account über den Link in der Mail („Sichere dein Konto hier“ oder „Secure your account here“) absichern. Achten Sie darauf, dass Sie auch tatsächlich auf https://www.instagram.com landen und nicht auf einer Phishing-Seite. Sie können über den Link ein neues Passwort setzen, das der Hacker nicht kennt. Überprüfen Sie von Zeit zu Zeit auch die „Login-Aktivität“ in den Sicherheitseinstellungen der App.

Informiert Sie Instagram ohne Ihr Zutun, dass Ihr Passwort oder die mit dem Account verknüpfte Mailadresse geändert wurde, sollten bei Ihnen die Alarmglocken läuten. Mit etwas Glück im Unglück können Sie aber auch in diesen Situationen die Kontrolle zurückgewinnen und die Änderung rückgängig machen, indem Sie in der Benachrichtigungsmail auf den Link „Sichere dein Konto hier“ klicken. Anschließend können Sie ein neues Passwort festlegen. Aber aufgepasst: Kontrollieren Sie auch in solch eiligen Fällen den Absender der Mail und das Ziel des Links genau, um sicherzustellen, dass es sich nicht um eine Phishing-Mail handelt. Geben Sie auf der verlinkten Seite nicht Ihr altes Instagram-Passwort ein.

Wurde der Account übernommen, kann ein Video-Selfie der letzte Ausweg sein.

Versteckter Rettungsweg

Für Härtefälle gibt es noch einen weiteren Rettungsweg über den Instagram-Support, der allerdings gut versteckt ist. Sie

erreichen ihn über die Instagram-App, indem Sie unterhalb des Login-Formulars auf „Erhalte Hilfe bei der Anmeldung“ tippen. Geben Sie oben Ihren Nutzernamen an und tippen Sie anschließend darunter auf „Du kannst dein Passwort nicht zurücksetzen?“. Die App fragt Sie daraufhin „Hast Du ein Foto von dir selbst in deinem Konto?“ – und das aus gutem Grund. Das Foto benötigt der Instagram-Support, um zu überprüfen, ob Sie der legitime Accountbesitzer sind. Falls Sie die Frage mit „Nein“ beantworten, ist Ihre Reise an dieser Stelle zu Ende und Sie landen im Hilfebereich.

Wenn Sie hingegen ein Foto in Ihrem Account haben und mit „Ja“ antworten, geht es weiter im Programm. Der genaue Ablauf variiert von Fall zu Fall. Instagram könnte Sie nach einem alten Passwort fragen und im darauffolgenden Schritt nach einem Bestätigungscode, den Sie sich an eine bei Instagram hinterlegte Mailadresse oder Handynummer schicken lassen können. Selbst wenn der Phisher die hinterlegten Daten geändert hat, stehen die Chancen gut, dass Sie hier noch Ihre wahre Rufnummer oder Mailadresse auswählen können und so an den Code kommen. Nach der Eingabe des Bestätigungscodes fragt Sie die App nach einer Mailadresse, über die Sie der Instagram-Support erreichen kann.

Video-Selfie

Haben Sie schließlich alle Hürden genommen, geht es ans Eingemachte: Die Instagram-App fordert Sie auf, Ihr Gesicht für ein sogenanntes Video-Selfie zu filmen. Im Rahmen dieses Vorgangs müssen Sie Ihren Kopf in vorgegebene Richtungen bewegen, um zu beweisen, dass Sie echt sind. Danach laden Sie das Video über den blauen „Senden“-Knopf hoch. Instagram beteuert, dass dieses Video maximal 30 Tage gespeichert wird und nicht zur Gesichtserkennung oder Speicherung biometrischer Merkmale genutzt wird. Wenn Sie das Video-Selfie hochgeladen haben, heißt es warten. Der Instagram-Support nimmt sich bis zu zwei Tage Zeit, um Ihr Anliegen zu bearbeiten.

Normalerweise geht es aber schneller. Nach der Überprüfung sendet Ihnen Instagram einen Link an die zuvor eingegebene Mailadresse, über den Sie ein neues Passwort festlegen können.

Falls Sie Ihren Facebook-Account mit Instagram verknüpft haben, gelten für diesen die gleichen Tipps: Nutzen Sie ein starkes Passwort, das nur bei Facebook passt, aktivieren Sie die Zwei-Faktor-Authentifizierung und achten Sie darauf, dass Ihre Kontaktdaten aktuell sind. Sie können zusätzlich die 2FA bei Instagram aktivieren, damit ein Angreifer, der bereits Kontrolle über Ihren Facebook-Account hat, nicht auch noch auf Ihr Instagram-Profil zugreifen kann.

Fazit

Instagram-Accounts stehen bei Cyber-Ganoven hoch im Kurs – insbesondere, aber nicht nur, wenn der begehrte blaue Haken das Profil ziert. Es ist daher wichtig, die Maschen der Angreifer zu kennen und frühzeitig geeignete Schutzmaßnahmen zu treffen. Wer sich nicht kümmert, riskiert sowohl, dass der Account gehackt wird, als auch, dass die vorhandenen Rettungsfunktionen ins Leere laufen, über die man die Kontrolle über einen gehackten Account zurückgewinnen könnte. *(rei@ct.de)*

1. Literatur
2. Ronald Eikenberg, E-Mails durchleuchtet, Phishing-Mails erkennen und abwehren, c’t 19/2022, S. 18
3. Niklas Dierking, Ronald Eikenberg, Schlosskombination, Verfahren und Geräte für sichere Online-Zugänge, c’t 9/2022, S. 18

Instagram-Hilfe zur Absicherung: ct.de/yqn6

QR-Codes – Sicherheitsprobleme

Gefahr im Bithaufen

QR-Codes: Sicherheitsproblem oder nicht?

QR-Codes können ähnlich wie Phishing-Mails Träger gefährlicher URLs sein. Wir erklären, welche Tricks sich Kriminelle ausgedacht haben und worauf Sie beim Scan von QR-Codes achten müssen.

Von Wilhelm Drehling

Die quadratischen Codes sind im Alltag nützliche Helfer: Mit einem Scan können Sie eine URL aufrufen, einen Kontakt hinzufügen oder dem Gast zu Hause das Abtippen des WLAN-Passworts ersparen. Weil sie praktisch sind und auch mal leichtfertig gescannt werden, haben auch Angreifer ihre Freude an QR-Codes gefunden. Denn das Aussehen des QR-Codes verrät nichts über dessen Inhalt, so kann sich in dem Pixelhaufen ein gefährlicher Link zu einer täuschend echten Anmeldeseite einer Fake-Bank oder zu einem Trojaner verbergen. In den vergangenen Jahren haben Kriminelle originelle Methoden erfunden – denen man aber zum Glück nicht schutzlos ausgeliefert ist.

Quishing

Das erste Angriffsszenario gehört in die Kategorie der Phishing-Angriffe: Vermutlich kommen Ihnen dubiose Mails wie „PayPal: Ihr Konto ist vorübergehend eingeschränkt“ bekannt vor. Mit solchen Mails versuchen die Angreifer häufig, an Ihre

Anmeldedaten heranzukommen, indem sie Sie auf eine gefälschte Webseite mit gewohntem Anmeldefenster weiterleiten. Enthält die Mail einen QR-Code, der zur Phishing-Seite führt, spricht man von Quishing.

Der große Unterschied zu den üblichen Mail-Betrügereien: Es hat sich bereits herumgesprochen, dass man nicht einfach so auf Links in Mails klicken sollte, die möglicherweise obendrein in schlechtem Deutsch verfasst sind. Bei QR-Codes ist das nicht der Fall. Ergo schenkt man QR-Codes mehr Vertrauen, scannt sie ein und landet dann womöglich auf einer Phishing-Seite oder Ärgerem.

Diese Masche tritt häufig in unterschiedlichen Varianten auf: Die Volksbank warnte im Dezember 2021 vor Mails und sogar Briefen mit QR-Codes, die Kunden dazu aufforderten, eine neue App herunterzuladen und sich dort zu registrieren. Ähnliche Angriffe mit QR-Codes häuften sich in letzter Zeit so sehr, dass die Polizei eine Warnung vor QR-Codes in Mails aussprach (sämtliche Warnungen haben wir Ihnen unter ct.de/yrf5 verlinkt).

Ob diese Warnungen wirklich etwas bringen, lässt sich diskutieren. Der c’t-Security-Experte Jürgen Schmidt geht in seinem Kommentar im Kasten rechts dieser Frage auf den Grund.

QR-Codes sind nicht das Problem

Ein Kommentar von Jürgen Schmidt (Leiter heise Security)

Die Krypto-Börse Coinbase platzierte in der Halbzeitpause des Superbowls einen Werbespot, der die Zuschauenden dazu verleiten sollte, einen über den Fernseher hüpfenden QR-Code

mit der Handy-Kamera einzufangen. Auf der dann angezeigten Website erwartete sie nur eine Meldung, dass der Dienst nicht erreichbar ist – vermutlich wegen Überlastung. Aber das ist eine andere Geschichte.

Es folgte ein Aufschrei der um die Sicherheit besorgten Experten, dass man den Anwendern unsichere Verhaltensweisen antrainiere und somit Phishing-Betrügern in die Karten spiele. Schließlich könne sich hinter dem QR-Code doch auch eine bösartige Phishing-Webseite verbergen, die es auf ihre Zugangsdaten abgesehen hat. Ich halte diesen Ansatz für falsch.

Das World Wide Web beruht darauf, dass Anwender Links öffnen. Auch solche, bei denen sie vorher nicht wissen, was genau sich dahinter verbirgt, schließlich will man ja Dinge entdecken. Es ist deshalb unsere (uns hier im Sinne von all denen, die im weitesten Sinne das Web mitgestalten) Aufgabe, den Anwendern Werkzeuge bereitzustellen, mit denen sie das tun können. Sprich: Anwender sollten einen Link ohne unmittelbare Gefahr öffnen können. Wenn allein durch das Öffnen eines Links etwas Böses passiert, dann ist das ein Fehler im Browser, den dessen Hersteller zu verantworten und zu beseitigen hat.

Die Verantwortung des Anwenders beginnt, wenn er mit der Seite interagiert. Bevor er dort persönliche Daten oder sogar ein Passwort eingibt, sollte er sich die Frage stellen, ob und wie weit er der Seite vertrauen kann. Da spielt primär der Kontext eine wichtige Rolle. Das ist in der analogen Welt nicht anders: Dem Hotel-Angestellten beim Check-in gibt man seine Kreditkarte; einem Unbekannten am Bahnhof eher nicht.

In der digitalen Welt zeigt sich da schon das erste Problem: Browser zeigen immer öfter gar nicht mehr an, wo sich der Anwender gerade befindet und machen es damit schwer, die Vertrauenswürdigkeit einer Passwortabfrage zu beurteilen oder gar zu überprüfen. Immerhin können sich Anwender fragen: Wie bin ich hierher gelangt? Über ein gespeichertes Lesezeichen

oder einen QR-Code in einem eher zweifelhaften Zusammenhang? Der Vertrauens-Check ist nicht trivial – aber etwas, was man Anwendern beibringen kann und sollte. „Klicke nicht auf Links“ oder „Verwende keine QR-Codes“ hingegen sind keine sinnvollen Lernziele. Darüber hinaus kann man Anwender zu Multifaktor-Authentifizierung und insbesondere FIDO2 ermuntern, weil sie konzeptionell vor Phishing schützen.

Eine Verteufelung von QR-Codes hingegen führt nur zu noch mehr angeblichen „Best Practices der Security“, die zwar gebetsmühlenartig wiederholt werden, an die sich niemand wirklich hält, weil sie praxisfern sind. Ich scanne den QR-Code im Restaurant, um mir die Speisekarte anzuschauen und ich würde mir wünschen, dass auch meine Bank Girocodes einführt [1], weil ich es satthabe, ständig gefühlt 100-stellige IBANs von Hand einzutippen. Ich werde also auch anderen Menschen, die sich von mir Sicherheitstipps erhoffen, nicht erzählen, dass sie keine QR-Codes benutzen dürfen, sondern lieber zur Zweifaktor-Authentifizierung raten.

Überklebt

Ein deutlich gefährlicherer und unscheinbarer Angriffsvektor geht von öffentlichen QR-Codes aus, die Sie in Broschüren, Werbeplakaten oder Speisekarten finden. Angreifer können die Codes überkleben und die Opfer somit auf gefälschte Webseiten locken. Die Idee hinter dem Angriff ist nicht neu, schon 2013 warnte das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor überklebten QR-Codes.

Das passiert nicht unbedingt bei Speisekarten; vorsichtig müssen Sie bei QR-Codes sein, die „alternative Bezahlmöglichkeiten“ anpreisen. Das FBI warnt in den USA zum Beispiel davor, keine QR-Codes bei Parkplätzen zu scannen, die zu einem Bezahldienst weiterleiten: Anstatt zum Parkautomat zu laufen, könne man so bequem die Rechnung für die Parkdauer bezahlen. Doof nur, wenn das Geld dann nicht an den Parkplatzbetreiber fließt, sondern direkt in die Taschen der

Betrüger.

Überklebte QR-Codes verheißen auch bei Außenwerbung Unheil, die dazu einlädt, eine App herunterzuladen oder Webseiten zu besuchen. In solchen Fällen greifen die Angreifer erneut nach Ihren Daten und im schlimmsten Falle versuchen sie, über eine App einen Trojaner auf Ihr Smartphone herunterzuladen (zugegebenermaßen ist das leichter beim Google Play Store zu bewerkstelligen als über den App Store auf iOS).

Genauso kritisch sind leicht zugängliche QR-Codes in Zügen oder Einkaufszentren, die einen einfachen Zugang zum WLAN anbieten: Ein solcher QR-Code kann von Angreifern überklebt worden sein. Mit einem Klick verbinden Sie sich mit einem von Angreifern eingerichteten gleichnamigen Hotspot.

Gegenmaßnahmen

Hersteller von Smartphones haben schon früh reagiert: Kamera-Apps folgen nicht mehr direkt einer gescannten URL. Ein Großteil aller modernen Kamera-Apps zeigt den Link stattdessen auf dem Bildschirm an. Danach ist es an Ihnen, zu entscheiden, ob Sie darauf klicken oder nicht. Dabei ist der gesunde Menschenverstand gefragt: Sieht die URL merkwürdig aus, dann sollten Sie den QR-Code genauso wie eine Phishing-Mail in den Papierkorb befördern.

Wenn Sie zusätzlich auf Nummer sicher gehen wollen (oder Familienangehörigen einen Gefallen tun wollen), weichen Sie unter Android auf eine App wie zum Beispiel Trend Micro QR-Scanner aus (siehe ct.de/yrf5), die den Inhalt des QR-Codes prüft und Sie vor potenziell gefährlichen Links warnt. iOS-Nutzer nehmen die App Intercept X von Sophos (siehe ct.de/yrf5). Die sichere Scanfunktion für QR-Codes ist aber nur ein kleiner Teil der Antiviren-App: Mit der App laden Sie leider noch viele weitere Funktionen herunter, deren Sinn mindestens zweifelhaft ist.

Mit der App QR-Scanner von Trend Micro bekommen Sie eine Einschätzung, ob die URL hinter dem QR-Code potenziell gefährlich ist.
Tipp für ganz harte Tüftler: Alternativ können Sie Ihr Smartphone beiseitelegen und den QR-Code per Hand dekodieren [2]. Das ist zwar mühsam, aber Sie fangen sich auf diese Art und Weise definitiv kein Virus ein.

Fazit

Wie bei vielen der vorgestellten Szenarien spielt der Kontext

eine wichtige Rolle: Ein QR-Code mit WLAN-Daten bei Ihnen zu Hause genießt ein höheres Vertrauen als ein QR-Code auf einem Laternenmast, der für ein öffentliches WLAN wirbt. Im Zweifel sollten Sie die Entscheidung, eine fragwürdige URL anzuklicken, dem gesunden Menschenverstand überlassen oder bei noch größeren Zweifeln eine QR-Überprüfungs-App konsultieren. *(wid@ct.de)*

1. Literatur
2. Jan Mahn, Schöner zahlen, Rechnungen schneller überweisen mit QR-Codes, c't 7/2022, S. 138
3. Wilhelm Drehling, Bithaufen, QR-Codes verstehen und ohne technische Hilfsmittel per Hand dekodieren, c't 17/2022, S. 142

Warnungen und Scanner-App: ct.de/yrf5