Kurz notiert – März 2023

Kurz notiert

Die Linux Foundation hat mit der **Open Metaverse Foundation** eine neue Unterorganisation gegründet. Die Stiftung soll Standards für ein herstellerneutrales Metaverse entwickeln.

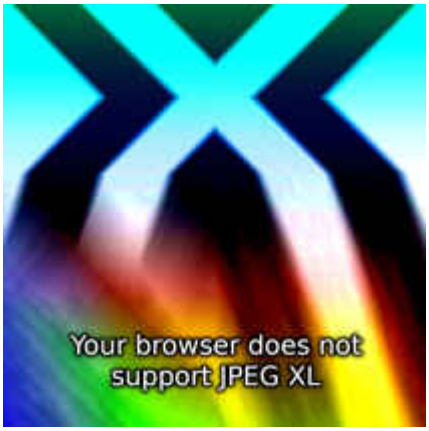
Die **Abmahnwelle wegen Google Fonts** hat in Österreich Schäden von mehr als 5 Millionen Euro verursacht. Darauf deutet die Einschaltung der Wirtschaftsstaatsanwaltschaft (WKSta) hin, die erst ab diesem Betrag aktiv wird.

Das **World Wide Web Consortium (W3C)** hat seine Umwandlung in eine gemeinnützige Non-Profit-Organisation abgeschlossen. Zuvor war das Konsortium ein Zusammenschluss von Bildungs- und Forschungseinrichtungen ohne eigenen Rechtsstatus.

Bei der aktuellen Firefox-Version 109 hat Mozilla die wegen Einschränkungen für Adblocker umstrittene **Plug-in-Schnittstelle Manifest V3** als Standard aktiviert. Manifest V2 ist aber noch vorhanden und wird von Mozilla unterstützt.

Mozilla Firefox: JPEG XL muss draußen bleiben

Wie bereits Chrome soll auch Firefox das Grafikformat JPEG XL nicht unterstützen. Mozilla hält dies nicht für notwendig, da es im Vergleich zu anderen Formaten zu wenig Vorteile biete.



Firefox wird das vielseitige und ressourcensparende

Grafikformat JPEG XL in absehbarer Zeit nicht darstellen. Das gab Mozillas Distinguished Engineer Martin Thomas auf der GitHub-Seite des Projekts bekannt. Man sei gegenüber dem Format „neutral“ – was bedeute, dass man es in stabilen Firefox-Versionen nicht erlaube, auch nicht optional, obwohl dies technisch mit wenig Aufwand möglich ist.

Mozilla unterstütze neue Formate nur, wenn sie Bedürfnisse der Nutzer und Websitebetreiber adressieren, so Thomas. JPEG XL habe zwar einige potenzielle Vorteile, sei aber gegenüber Mitbewerbern wie AVIF nicht so viel performanter und vielseitiger, dass es die Aufnahme in den Browser rechtfertige. Damit übernimmt Thomas das Argument, das bereits führende Chrome-Entwickler ins Feld führten. Google hatte sich im Herbst 2022 dagegen entschieden, das Format in seine Browser-Engine aufzunehmen.

Befürworter argumentieren damit, dass JPEG XL die bessere Alternative sowohl für klassische Pixel-Formate wie JPEG und PNG als auch für die von Videocodecs abstammenden animationsfähigen Standards wie WebP oder AVIF sei. Auch hatten sich in der Vergangenheit Unternehmen wie Intel, Adobe, Meta oder Shopify hinter das Format gestellt. Bisher können bei den Browsern nur Nischenprodukte JPEG-XL-Dateien anzeigen, darunter Firefox-Derivate wie Waterfox oder Pale Moon. (ulw@ix.de)

Browser-Engine Servo mit neuer Finanzierung nach langer Pause wiederbelebt

Nach über zwei Jahren ohne nennenswerte Aktivitäten hat das Entwicklerteam der Browser-Engine Servo die Arbeit wieder aufgenommen. In einem Blogbeitrag kündigten die Entwickler eine neue externe Finanzierung an, die die Fortführung ermögliche – ohne jedoch die Geldgeber zu nennen. Bereits im Dezember hatte die Entwicklergenossenschaft Igalia bekannt gegeben, dass sich vier ihrer Mitarbeiter künftig der Weiterentwicklung von Servo widmen werden. Bei Igalia arbeiten

renommierte Browserspezialisten, die zu den verbreiteten Engines Chromium und WebKit wichtige Beiträge leisten.

Servo ist eine in Rust implementierte Browser-Engine, die 2012 als Mozilla-Projekt an den Start ging. Sie sollte im Rahmen des Projekts Quantum in Firefox integriert werden, dazu kam es jedoch nie. 2020 wanderte Servo in der Folge einer Entlassungswelle bei Mozilla zur Linux Foundation, aber auch dort schlief die Aktivität bald wieder ein.

Jetzt gibt es eine neue Roadmap für 2023. In diesem Jahr sollen neben Aufräumarbeiten bei den Dependencies das Layoutsystem und die Umsetzung von CSS2 im Fokus stehen. (ulw@ix.de)

Malvertising-Welle bei Google-Suchen

Mehrere Sicherheitsforscher beobachten einen starken Anstieg von Malvertising über Google Ads. Immer mehr der bei Google-Suchen eingeblendeten Anzeigen verlinkten auf Schadsoftware statt auf beliebte Programme wie Adobe Reader, Slack, Gimp oder Thunderbird. Securityexperten bei Spamhaus vermuten, dass eine Cybercrime-Gruppe damit begonnen hat, Malvertising als Service zu vermarkten. Ein Hinweis darauf sei unter anderem, dass bei gleichlautenden Suchbegriffen Links auf unterschiedliche Schädlinge auftauchen.

Die Securityfirma SentinelOne hat eine Malware-Kampagne identifiziert, die auf bösartige Loader für .NET verlinkt. Am häufigsten versuchen die Angreifer derzeit, XLoader zu installieren, einen Nachfolger von FormBook, der Passwörter, Kontaktdaten und andere sensible Informationen stiehlt. (ulw@ix.de)

Chrome-Updates nur noch ab Windows 10

Mit dem Erscheinen von Chrome in Version 110 bekommen die Versionen für Windows 7, 8 und Windows Server 2012 keine Sicherheitsupdates mehr. Microsoft hat den erweiterten Support

für diese Betriebssysteme bereits ab Januar eingestellt. In Chrome 110 hat Google 15 Sicherheitslücken geschlossen, drei davon mit Risikoeinstufung „hoch“.

Mit Version 110 von Chrome kommt es zu einer Änderung im Releasezyklus. Künftig gibt es für ausgewählte Nutzer eine Early-Stable-Version, die eine Woche vor dem eigentlichen stabilen Release erscheint. Google will damit in der Lage sein, noch vor dem Veröffentlichen der stabilen Version auf Probleme bei Anwendern zu reagieren. (ulw@ix.de)

Markt + Trends | World Wide Web

Gravierende Mängel beim Kündigungs-Button

Seit dem 1. Juli 2022 müssen in Deutschland tätige Unternehmen den sogenannten Kündigungs-Button auf ihren Webseiten anbieten. Die Verbraucherzentrale Bayern hatte systematisch Webseiten überprüft und bei der Mehrheit davon erhebliche rechtliche Mängel aufgedeckt. Ein Großteil bewegte sich überdies im Graubereich, teilt die Verbraucherzentrale Bayern mit.

Die Verbraucherverbände hätten insgesamt 152 Unternehmen abgemahnt. Lediglich auf 273 von 840 überprüften Websites fanden sich gesetzeskonforme Kündigungs-Buttons, heißt es aus Bayern weiter.

349 Webseiten ließen den vorgeschriebene Kündigungs-Button ganz vermissen. In 65 Fällen war er auf der Website versteckt, in 38 Fällen trug er eine unzulässige Beschriftung. Überdies wurden 339 weitere Verstöße im Zusammenhang mit der Bestätigungsseite und dem finalen Bestätigungs-Button festgestellt, teilen die Verbraucherschützer mit. Es hätten zum Beispiel Pflichtangaben gefehlt, oder es habe unzulässige Beschriftungen gegeben. Letztere müssen ebenfalls bestimmten Formalien genügen.

Bis Anfang November 2022 zeigten sich 86 Unternehmen einsichtig und unterschrieben die geforderte Unterlassungserklärung. In drei Fällen erwirkten die Verbraucherschützer eine einstweilige Verfügung, in 17 Fällen haben sie ein Klageverfahren vorbereitet oder bereits ein solches eingereicht.

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

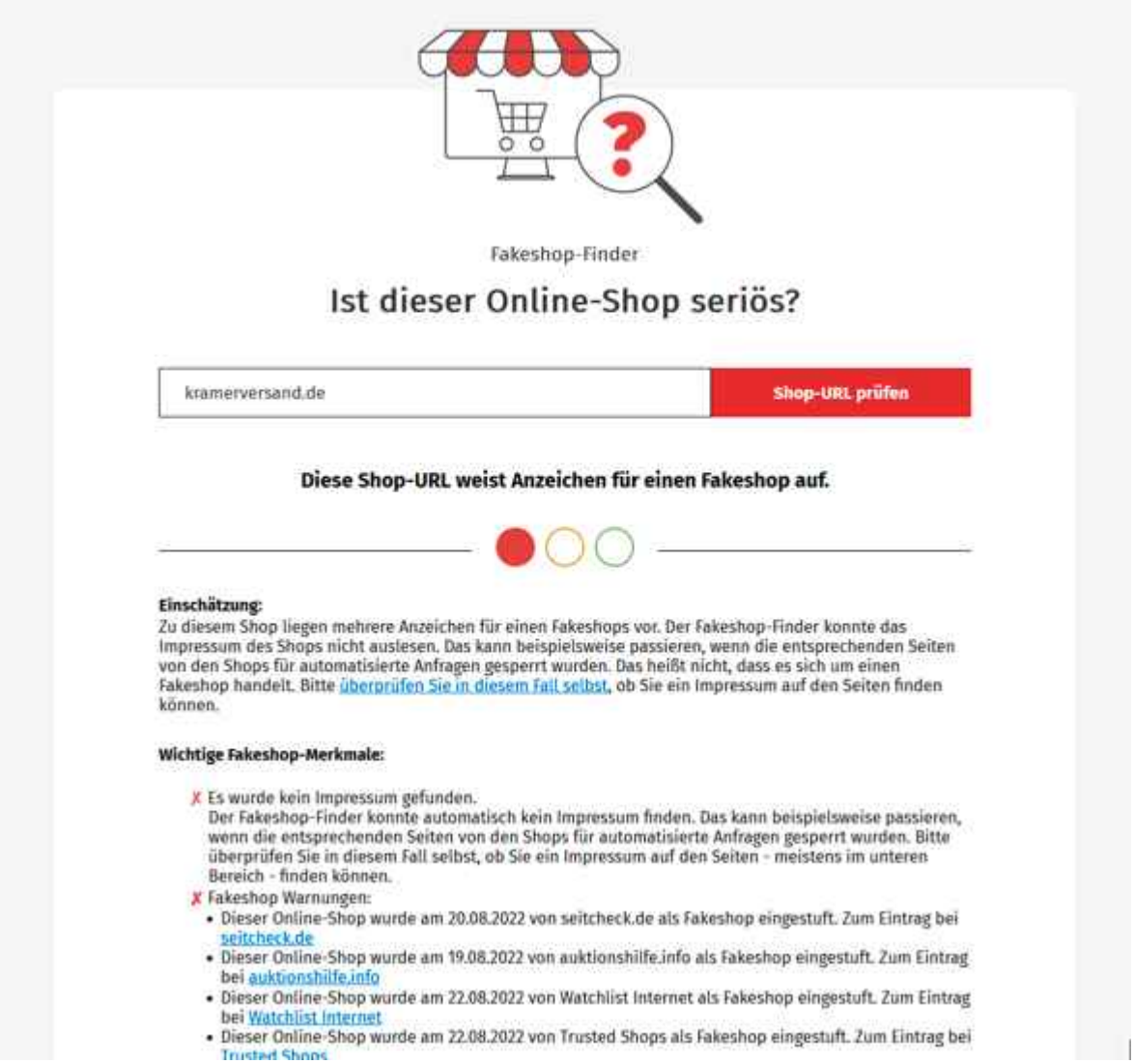
Als Zahlart bieten viele Fake-Shops ausschließlich Vorkasse per Banküberweisung an, da man solche Zahlungen in der Regel nicht rückgängig machen kann. Mitunter wollen betrügerische Händler Kunden auch gerne zu PayPal-Zahlungen in der Variante „Freunde und Familie“ verleiten. Die beinhalten aber im Unterschied 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

Ungepatchte Schwachstelle im WordPress-Core: Was es wirklich bedeutet

Geschrieben von iThemes-Redaktionsteam an 14. Dezember 2022

Zuletzt aktualisiert am 14. Dezember 2022

Diese Woche Im iThemes Vulnerability Report werden Sie feststellen, dass es eine ungepatchte Schwachstelle im WordPress-Core gibt. Diese Schwachstelle wurde von Thomas Chauchefoin gemeldet und betrifft derzeit alle Versionen von WordPress. Die wahrscheinliche Ausnutzung dieser Schwachstelle ist jedoch sehr gering, und um sich vollständig zu schützen, müssen Sie lediglich XML-RPC oder Pingbacks auf Ihrer WordPress-Site deaktivieren.

Was diese Schwachstelle für Ihre Website bedeutet

Obwohl ein vollständiger Proof of Concept noch nicht von WPScan veröffentlicht wurde, können wir einige fundierte Vermutungen darüber anstellen, wie diese Schwachstelle ausgenutzt werden kann. Sie sagen:

> *„WordPress ist von einer nicht authentifizierten blinden SSRF in der Pingback-Funktion betroffen. Aufgrund einer TOCTOU-Rennbedingung zwischen den Validierungsprüfungen und der HTTP-Anfrage können Angreifer interne Hosts erreichen, die ausdrücklich verboten sind.“*

Um diese Schwachstelle auszunutzen, würde ein Angreifer WordPress-Pingbacks verwenden, wäre aber dazu gezwungen, dies in Kombination mit anderen Schwachstellen zu tun.

Um eine Schwachstelle wie diese auszunutzen, um einer WordPress-Site irgendeinen Schaden zuzufügen, wäre diese Schwachstelle nur nützlich, wenn sie mit anderen ernsteren Schwachstellen auf einer nicht gepatchten oder unsicheren WordPress-Site verwendet wird.

Offiziell hat das Sicherheitsteam von WordPress.org erklärt, dass es sich um eine Schwachstelle mit niedriger Priorität handelt. Insbesondere sagten sie dem Daily Swig :

> *„… dies ist ein Problem mit geringen Auswirkungen, und um es auszunutzen, muss es mit zusätzlichen Schwachstellen in Software von Drittanbietern [verkettet] werden. Daher betrachtet das Sicherheitsteam das Problem als gering.“*

Sie fügten hinzu: „Aufgrund seines geringen Schweregrades diskutiert das Team, ob dieses Problem als allgemeine Härtungsmaßnahme öffentlich behoben werden könnte.“

Dies unterstreicht die Schwierigkeit, Sicherheitsfixes zu so vielen älteren Versionen von WordPress hinzuzufügen. Jahrelang hat das Kernteam Patches auf Versionen zurückportiert, die viele Jahre alt waren und nur von wenigen Nachzüglerseiten verwendet wurden, die noch nicht aktualisiert wurden. Die jüngste Entscheidung des Kernteams, ältere Versionen nicht mehr zurückzuportieren, wird die Behebung dieser Art von Problemen für das WordPress-Kernteam einfacher und schneller

machen.

So schützen Sie Ihre Website

Da Pingbacks der offensichtliche Schwachpunkt sind, der diskutiert wird, ist das Deaktivieren von Pingbacks und/oder XML-RPC ein guter erster Schritt.

Wenn Sie Ihre WordPress-Site auf dem neuesten Stand halten und sich auf einem zuverlässigen Hosting mit einer starken und sicheren Infrastruktur befinden, ist die Wahrscheinlichkeit einer Ausnutzung dieser Schwachstelle extrem gering.

Wenn Sie Ihre Website so sicher wie möglich halten möchten, ist es am besten, Pingbacks oder XML-RPC zu deaktivieren. Glücklicherweise bietet Ihnen iThemes Security die Möglichkeit, beides zu tun.

So deaktivieren Sie XML-RPC mit iThemes Security

Das Deaktivieren von XML-RPC mit iThemes Security ist unglaublich einfach. Gehen Sie zu **Sicherheit > Einstellungen > Erweitert > WordPress-Optimierungen** und verwenden Sie dann das Dropdown-Menü, um XML-RPC zu deaktivieren.

Es kann Fälle geben, in denen Sie XML-RPC benötigen. Diese beinhalten:

- Wenn Sie eine alte Website haben, die Sie nicht auf Version 4.4 oder höher aktualisieren können, haben Sie keinen Zugriff auf die REST-API und verwenden möglicherweise Dienste, die XML-RPC erfordern.
- Sie verwenden ein Programm, das nicht auf die REST-API zugreifen kann, um mit Ihrer Website zu kommunizieren.
- Integration mit einigen Apps von Drittanbietern, die nur

XML-RPC verwenden können.

Das Deaktivieren von XML-RPC ist mit iThemes Security ein einfacher Vorgang. Sie können dies ausschalten und die Funktionalität Ihrer Website testen, und wenn etwas nicht richtig zu funktionieren scheint, können Sie es wieder einschalten.

Dies sind Situationen, in denen es sinnvoll ist, einen Staging-Server einzurichten, damit Sie Änderungen testen können, bevor Sie sie auf Ihre Produktionssite anwenden.

Stummschalten der Schwachstelle in Ihrem iThemes Site Scan

Natürlich benachrichtigt Sie der Site-Scanner von iThemes Security über diese Schwachstelle. Da es in naher Zukunft nicht vom Kernteam behoben wird, könnte es sinnvoll sein, der Warnungsermüdung vorzubeugen, indem diese Schwachstelle im Site-Scanner stummgeschaltet wird. Weitere Informationen zum Stummschalten von Schwachstellenwarnungen finden Sie in unserer Hilfedokumentation .

Fazit

Obwohl diese Sicherheitsanfälligkeit nicht gepatcht ist, stellt sie ein sehr geringes Risiko für Besitzer von WordPress-Sites dar. Wenn auf Ihrer Website XML-RPC bereits deaktiviert ist, sind Sie bereits geschützt. Pingbacks sind eine der Legacy-Funktionen von WordPress, die in einigen Fällen nützlich sein können, aber es ist keine Funktion, die von vielen modernen Websites verwendet wird. Dies ist einer der Fälle, in denen es hilfreich ist, ein Sicherheits-Plugin wie iThemes Security installiert zu haben, damit Sie schnell Maßnahmen ergreifen können, um Ihre Website gegen Angreifer zu schützen, selbst wenn die betreffende Schwachstelle von

geringer Schwere ist.

Kartellamt: Google dominiert die Online-Werbe-Wertschöpfungskette

Kartellamt: Google dominiert die Online-Werbe-Wertschöpfungskette

Das Bundeskartellamt nimmt Google verstärkt ins Visier. Die Behörde erwägt in einem Bericht „breiter angelegte, möglicherweise strukturelle Eingriffe“, die über Einzelmaßnahmen hinausgehen.

Das 232 Seiten starke Diskussionspapier des Bundeskartellamts erklärt die verschiedenen Werbeformen und Geschäftsmodelle im Detail.

Das Bundeskartellamt hat in einem Diskussionsbericht dargestellt, wie es den nicht an Suchmaschinen gebundenen Teil des Online-Werbemarktes einschätzt. Dabei handelt es sich zum Beispiel um die Banner, die viele Medienangebote (mit-)finanzieren. Allein in Deutschland werden laut dem Bericht pro Jahr vier bis fünf Milliarden Euro mit solcher Werbung umgesetzt. Dahinter stecke ein „hochkomplexes, für viele recht intransparentes System des automatisierten Handels mit Online-Werbeplätzen“, das der Bericht auf etlichen Seiten erklärt.

Im Rahmen der Untersuchung, so die Wettbewerbshüter, habe sich vor allem die Vormachtstellung Googles gezeigt: „Google ist auf nahezu allen Stufen der Wertschöpfungskette und bei

praktisch allen relevanten Dienstleistungen vertreten und hat dabei in den meisten Fällen eine sehr starke Marktposition inne.“ Das Unternehmen kontrolliere wichtige Teile der nutzerseitigen Software-Infrastruktur wie den Browser Chrome und das mobile Betriebssystem Android. Damit bestimme es letztlich über die technischen Möglichkeiten mit, um Online-Werbung zu realisieren.

Der Bericht beurteilt nicht, ob Google seine Dominanz wettbewerbsschädigend ausnutzt, das Kartellamt will das aber weiter prüfen. Generell habe es neue Instrumente an die Hand bekommen, mit denen es gut gegen einzelne Praktiken vorgehen könne. Dazu zählt Andreas Mundt, der Präsident des Amts, den relativ neuen Paragrafen 19a des Gesetzes gegen Wettbewerbsbeschränkungen und den europäischen Digital Markets Act.

Bei Google könnte es aber nicht reichen, an einzelnen Stellschrauben zu drehen. Hier spricht der Bericht über „breiter angelegte, möglicherweise strukturelle Eingriffe“ – ohne diese weiter auszuführen. Das Bundeskartellamt ermöglicht es Marktteilnehmern und interessierten Kreisen, bis zum 28. Oktober 2022 Stellung zu dem Bericht zu beziehen. (jo@ct.de)

Podcasts bei YouTube und Twitter

YouTubeist bereits riesiger Anbieter von (Video-) Podcasts. Dieses Geschäft will die Plattform anscheinend weiter ausbauen, denn unter der URL youtube.com/podcasts **bietet YouTube gezielt Podcasts an**. Bis Redaktionsschluss war die Seite allerdings nur in den USA verfügbar; wann sie in Deutschland freigeschaltet wird, ist unklar.

Ebenfalls zunächst nur in den USA verfügbar ist eine neue Podcast-Funktion bei Twitter. Podcaster können ihre Sendungen dort veröffentlichen. Mit der Neugestaltung **führt Twitter personalisierte Hubs für Nutzer ein**, die sogenannten Stations. Sie gruppieren mehrere Inhalte auf Basis verschiedener Themen

wie Nachrichten, Musik und Sport. (jo@ct.de)

Post: Digitaler Briefversand nun bei 1&1

Die Post kooperiert mit Web.de und GMX beim digitalen Briefversand. Inhaber eines E-Mail-Kontos bei den 1&1-Diensten GMX und Web.de können künftig Briefe digital aus einem neuen Online-Office heraus an die Deutsche Post übermitteln. Dort werden sie ausgedruckt, frankiert und auf dem Postweg als gedruckter Brief an die Empfängeradresse zugestellt. Der Dienst ist bis Jahresende für monatlich drei Briefe pro E-Mail-Konto gratis. Was er danach kosten wird, steht noch nicht fest.

Parallel zur Einführung des neuen Dienstes stellt die Deutsche Post ihren eigenen Service „E-Post“ für Privatkunden bis Ende November 2022 ein. Für Geschäftskunden werde E-Post als Plattform zur Digitalisierung der Briefkommunikation hingegen unverändert fortgeführt und weiter ausgebaut. (jo@ct.de)