So richten Sie eine WordPress-Staging-Site mit BackupBuddy-Bereitstellung ein

Zuletzt aktualisiert am 7. Januar 2020

BackupBuddy Deployment ist eine neue Funktion in BackupBuddy 6.0, mit der Sie Änderungen einfach zwischen zwei WordPress-Sites übertragen oder ziehen können. In diesem Beitrag behandeln wir, wie Sie eine WordPress-Staging-Site mit dem WordPress-Backup-Plugin BackupBuddy einrichten.

Mit der Bereitstellung in BackupBuddy können Sie die Datenbank, Mediendateien, Plugins und das aktive Design einer WordPress-Site zwischen einer Staging-Site (oder Test-/Entwicklungssite) und einer Live-Site hin und her verschieben oder ziehen, sodass Sie auf einer Site und dann entwickeln können Push-Änderungen auf eine andere übertragen, sodass Sie nie wieder auf einer Live-Site entwickeln müssen.

Verwenden einer WordPress-Staging-Site in Ihrem WordPress-Entwicklungsworkflow

WordPress Staging ist eine Methode zur Entwicklung von WordPress-Websites an einem anderen Ort als Ihrer Live-WordPress-Site. WordPress-Staging kann aus zwei oder drei separaten Websites mit separaten URLs bestehen.

Beispielsweise haben Sie möglicherweise eine Staging-Site (Test-Site) und eine Live-Site (Produktions-Site).

- **Beispiel:** Sie könnten Ihre Site der Einfachheit halber lokal auf Ihrem Computer entwickeln und sie dann auf der Staging-Site (Test) auf demselben Server (aber unter einer anderen URL) wie die Live-Site bereitstellen, um sie Clients vorzuführen oder die Serverkompatibilität sicherzustellen usw. Sobald Sie zufrieden sind, können Sie die Änderungen an die Live-Produktionsseite übertragen.
- **Beispiel:** Wenn Sie ein größeres Plugin-Update ausprobieren möchten, sich aber vergewissern möchten, dass es die Live-Site nicht beschädigt, können Sie zu Ihrer Staging-Site gehen und dann die Live-Site herunterziehen. Nachdem Sie überprüft haben, dass alles wie erwartet funktioniert, können Sie die Änderungen entweder auf die Live-Site zurückschieben oder direkt zur Produktions-Site gehen und das Plugin dort aktualisieren.

Stellen Sie mit BackupBuddy Deployment mit wenigen Klicks Änderungen von einer Staging-Site auf eine Live-Site bereit

BackupBuddy verwendet ein neues Remote-Ziel „BackupBuddy Deployment“, um Ihre WordPress-Staging-Site und Ihre Live-Site zu verbinden. Wenn Sie den Bereitstellungsprozess einleiten, werden die Inhalte der Zielsite (der Site, auf die Sie pushen) nach Bedarf überschrieben.

Während der Bereitstellung wird Ihnen ein kontinuierlicher Status des Prozesses angezeigt und Sie haben die Möglichkeit, die Änderungen zu testen und die Datenbankänderungen

rückgängig zu machen, bevor Sie sie dauerhaft machen.

- Sehen Sie sich vor der Bereitstellung Unterschiede in den Standortservereinstellungen, aktiven Plugins, Designs, Versionen und Medien an.
- Optionen zum Übertragen der Datenbank (alle Tabellen, einige oder keine), Plugins, Design und/oder Medien.
- Automatische Migration von URLs, Pfaden und anderen Einstellungen genauso wie manuelle Migrationen.
- Beobachten Sie den Bereitstellungsfortschritt genau wie bei einem normalen Backup und zeigen Sie einen kontinuierlichen Status an, einschließlich eines detaillierten erweiterten Statusprotokolls des gesamten Prozesses, alles an einem Ort.
- Möglichkeit, die Datenbankänderungen mit einem Klick rückgängig zu machen, wenn etwas schief geht, bevor Sie die Bereitstellung bestätigen, sobald Sie zufrieden sind.
- Automatisches Aufteilen von Daten, die zwischen Servern übertragen werden, um große Dateien oder langsame Server zu unterstützen.
- Tauscht Datenbanken erst aus, nachdem die gesamte Datenbank und alle Dateien übertragen wurden, um zu versuchen, die Ausfallzeit der Site auf wenige Sekunden (oder weniger!) zu minimieren.
- Perfekt für die Entwicklung Ihrer Website an einem anderen Ort als der Live-Website. Verwenden Sie Best Practices für die Bereitstellung.

So richten Sie eine WordPress-Staging-Site mit BackupBuddy-Bereitstellung ein

Die superschnelle Version dieses Tutorials sieht ungefähr so aus:

1. Erstellen Sie eine Sicherungskopie Ihrer Live-Site.
2. Erstellen Sie eine Staging-(Test-)Site, indem Sie Ihr Backup auf einer neuen Domain wiederherstellen (z. B. dev.yourdomain.com).
3. Füge **define(‚BACKUPBUDDY_API_ENABLE', true) hinzu;** in die Datei wp-config.php deiner Live-Site.
4. Gehen Sie auf der Live-Site zu **BackupBuddy > Remote-Ziele** und **wählen Sie** oben auf der Seite Bereitstellungsschlüssel anzeigen aus
5. Kopieren Sie den angegebenen Schlüssel.
6. Gehen Sie auf Ihrer Staging-Site zu **BackupBuddy > Remote-Ziele** und **klicken Sie auf die Option Neu** hinzufügen und wählen Sie dann **BackupBuddy-Bereitstellung.**
7. **Fügen Sie den API-Schlüssel** , den Sie von der Live-Site kopiert haben, in Ihre Staging-Site ein.

Die längere, ausführlichere Version dieses Tutorials:

1. Gehen Sie auf Ihrer Live-Site **zu BackupBuddy > Remote Destinations** und wählen Sie dann die Schaltfläche „ **Show Deployment Key** " oben auf der Seite.

Wenn Sie die Bereitstellung auf dieser Site zum ersten Mal einrichten, werden Sie aufgefordert, die folgende Zeile zur Datei wp-config.php Ihrer Live-Site hinzuzufügen. define(‚BACKUPBUDDY_API_ENABLE', true);

Nachdem du diese Zeile zu deiner wp-config.php-Datei deiner Live-Site hinzugefügt hast, aktualisiere die Seite und **wähle erneut „Bereitstellungsschlüssel anzeigen"** , um den Schlüssel anzuzeigen). Sie sehen einen Bereitstellungs-API-Schlüssel, der ungefähr so aussieht:

eyJrZXlfdmVyc2lvbiI6MSwia2V5X3B1YmxpYyI6IjXiMzJmZjJmZjEzODhlOWRmNzA5YzFkY2NkYzNlMzY2Iiwia2V5X3NlY3JldCI6IjM5ZWM1NWE3YjJiZmY3OWIwYTAyOTNlZmYxMxODczIiwia2V5X2NyZWF0ZWQiOjE0MjExMTAwOTUsInNpdGV1cmwiOiJodHRwsdml84sC9iYWNrdXBidWRkeTIiLCJob21ldXJsIjoiaHR0cDpsdjc98wjDXXYaVwYnVkZHkyIn0=

2. Kopieren Sie diesen Schlüssel. Sie geben diesen Schlüssel in Ihre Staging-Site ein.

3. Gehen Sie auf Ihrer Staging-Site zur **Seite BackupBuddy > Remote-Ziele** und klicken Sie auf die Registerkarte „ **+ Neu hinzufügen.** ” Wählen Sie das Ziel „BackupBuddy Deployment“.

4. Geben Sie den API-Schlüssel ein, den Sie von Ihrer Live-Site kopiert haben. Sie können das Ziel jetzt testen und hinzufügen. Die Einrichtung ist jetzt abgeschlossen!

Push & Pull von Änderungen von der Staging-Site zur Live-Site

1. Gehen Sie zu der Site, von der Sie Pushen oder Pullen möchten.

2. Gehen Sie zur **Seite BackupBuddy > Remote-Ziele** und wählen Sie die **Registerkarte „Meine Bereitstellungssite“** , die Sie während des Setups hinzugefügt haben.

3. Wählen Sie „Push to“ oder „Pull from“, je nachdem, was Sie tun möchten.

4. Ihnen werden Informationen zu beiden Seiten und deren Serverkonfiguration angezeigt, einschließlich WordPress- und Plugin-Versionen, Medieninformationen, Datenbanktabellen,

Laufzeitdetails und mehr.

5. Wählen Sie aus, welche Daten Sie übertragen möchten, einschließlich Datenbanktabellen, Mediendateien, Plugins und Designdateien.

6. **Klicken Sie auf „Begin Push/Pull“** , um den Vorgang zu starten. Sie erhalten eine Statusanzeige, die einen Überblick über den aktuellen Fortschritt einschließlich der übertragenen Dateien einschließlich eines detaillierten Statusprotokolls gibt.

7. Testen Sie die Zielseite, um sicherzustellen, dass alles in Ordnung aussieht, und klicken Sie dann auf **„Änderungen bestätigen“** , um diese Änderungen abzuschließen. Wenn Sie die Änderungen nicht innerhalb von 12 Stunden bestätigen, gelten sie als abgeschlossen.

Wenn Sie mit den Änderungen nicht zufrieden sind, wählen Sie „Datenbankänderungen rückgängig machen“, um auf die Datenbank zurückzusetzen, die vor dem Bereitstellungsprozess vorhanden war.

Um eine Zusammenfassung der übertragenen Dateien anzuzeigen, besuchen Sie die **Seite BackupBuddy > Remote-Ziele** erneut. Von hier aus können Sie Übertragungs- und Statusinformationen anzeigen.

Staging Best Practices

Beim Pushen und Pullen zwischen Sites ist es wichtig, dass Sie nur die Inhalte senden, die Sie auf der Zielsite überschreiben möchten. Zum Beispiel möchten Sie wahrscheinlich darauf verzichten, die WordPress-Kommentare auf Ihrer Entwicklungsseite an Ihre Produktionsseite zu senden, damit

Kommentare nicht überschrieben werden.

BackupBuddy führt keine Datenbankinhalte „zusammen“. Ganze Tabellen werden entweder gesendet oder nicht gesendet. Sie können etwas Ähnliches wie bei einer Zusammenführung tun, indem Sie eine oder mehrere Tabellen von der Bereitstellung ausschließen. Nicht gesendete Tabellen führen dazu, dass die vorhandene Datenbanktabelle unverändert bleibt.

Weitere wichtige Hinweise zur Bereitstellung von BackupBuddy

- Mindestens eine Website muss auf die andere URL zugreifen können. Zum Pushen muss diese Ziel-URL beispielsweise vom Quellcomputer aus zugänglich sein.
- Nur aktive Designdateien werden aktualisiert und beide Sites müssen zu diesem Zeitpunkt dasselbe aktive Design haben.
- Sites müssen über genügend Ressourcen verfügen, um Dateien sichern, wiederherstellen und Verbindungen zum Senden von Dateien (z. B. über curl) herstellen zu können. BackupBuddy sollte für die normale Funktionalität voll funktionsfähig sein, bevor Sie Bereitstellungen versuchen.
- Beim Übertragen von Dateien dürfen Dateien, die auf dem anderen Server gelöscht wurden, nicht aus der Ferne gelöscht werden.
- Beim Übertragen von Dateien werden leere Verzeichnisse nicht übertragen.
- Die Windows-Unterstützung ist derzeit experimentell und wird derzeit nicht unterstützt. Die Unterstützung für die Windows-Bereitstellung ist in Bearbeitung.
- Es wird empfohlen, dass der Remote-Server einen Admin-Benutzer mit demselben Benutzernamen wie der lokale Server hat. Wenn dies nicht der Fall ist, kann beim Abrufen des Servers nach der Wiederherstellung eine

Abmeldung erfolgen. Wir versuchen, dies zu umgehen, aber einige Setups können dennoch zu einer Abmeldung führen.

Holen Sie sich jetzt BackupBuddy mit Bereitstellung

Beschleunigen Sie Ihren WordPress-Entwicklungsworkflow mit Deployment in BackupBuddy, dem 3-in-1- Plugin für WordPress-Backups . Zusätzlich zur Bereitstellung bietet BackupBuddy eine Menge anderer entwicklungsorientierter Funktionen, wie die WordPress-Migration , die Möglichkeit, WordPress zu klonen und mehr.

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

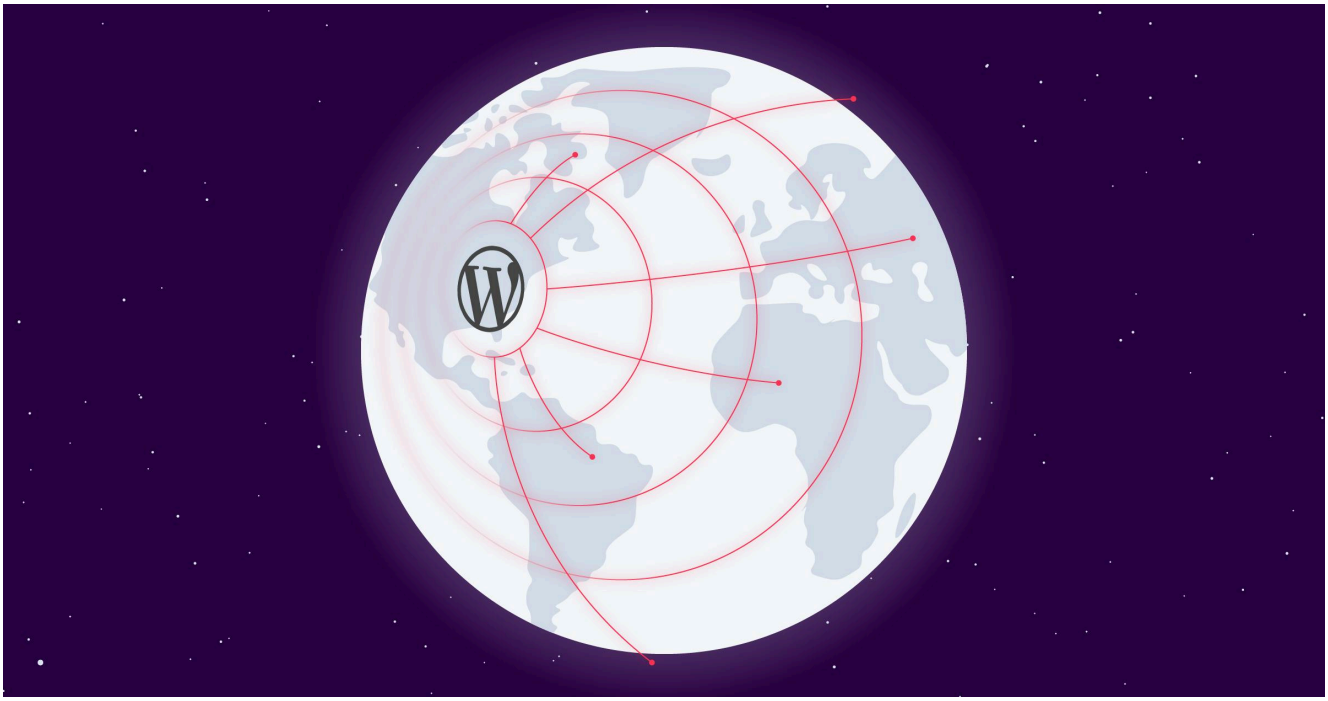
Natürlich benachrichtigt Sie der Site-Scanner von iThemes Security über diese Schwachstelle. Da es in naher Zukunft nicht vom Kernteam behoben wird, könnte es sinnvoll sein, der Warnungsermüdung vorzubeugen, indem diese Schwachstelle im Site-Scanner stummgeschaltet wird. Weitere Informationen zum Stummschalten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

WordPress Core – Unauthenticated Blind SSRF



WordPress Core – Unauthenticated Blind SSRF

Our security researchers were surprised to discover a low-hanging code vulnerability in WordPress Core that we will discuss in this blog post.

by simon scannell and thomas chauchefoin|September 06, 2022

WordPress ist das weltweit beliebteste Content-Management-System und wird von über 40 % aller Websites verwendet . Diese breite Akzeptanz macht es zu einem Top-Ziel für Bedrohungsakteure und Sicherheitsforscher, die für das Melden von Sicherheitsproblemen über ihr öffentliches Bug-Bounty-Programm bezahlt werden.

Vulnerability Broker sind auch sehr daran interessiert, ungepatchte Schwachstellen zu erwerben, die es ihnen ermöglichen, WordPress-Instanzen zu übernehmen, und bieten manchmal bis zu 300.000 US-Dollar für kritische Schwachstellen. Als solches hat WordPress eine stark überprüfte Codebasis, in der von Forschern nicht mehr erwartet wird, dass sie niedrig hängende Früchte finden. Unsere bisherigen Recherchen zu diesem Ziel erforderten umfangreiche Fachkenntnisse und Anstrengungen, um Sicherheitsprobleme aufzudecken.

Dieser Blogbeitrag beschreibt eine überraschend einfache Schwachstelle in der WordPress-Implementierung von Pingbacks. Während die Auswirkungen dieser Schwachstelle im Falle von WordPress für die meisten Benutzer gering sind, ist das damit verbundene anfällige Codemuster ziemlich interessant zu dokumentieren, da es wahrscheinlich auch in den meisten Webanwendungen vorhanden ist. Das Ziel dieses Blogbeitrags ist es, über dieses Muster aufzuklären und das Bewusstsein zu schärfen.

Offenlegung

Diese Schwachstelle wurde WordPress am 21. Januar gemeldet; es ist noch keine Lösung verfügbar. Bitte lesen Sie den Abschnitt *Patch* , um eine Anleitung zu möglichen Korrekturen zu erhalten, die Sie auf Ihre WordPress-Instanzen anwenden können.

Es ist das erste Mal, dass wir Details über eine ungepatchte Schwachstelle veröffentlichen, und diese Entscheidung wurde uns nicht leicht gemacht. Dieses Problem wurde erstmals vor etwa sechs Jahren im Januar 2017 von einem anderen Forscher und zahlreichen anderen im Laufe der Jahre gemeldet. Nach unserem Bericht und weiteren Untersuchungen konnten wir auch mehrere öffentliche Blog-Posts identifizieren, die dasselbe Verhalten dokumentieren wie der, über den wir heute berichten werden.

Aufgrund der geringen Auswirkungen in der vorliegenden Form, der vorherigen Veröffentlichung und der Notwendigkeit, sie mit zusätzlichen Schwachstellen in Software von Drittanbietern zu verketten, glauben wir, dass diese Version WordPress-Benutzer nicht gefährdet und ihnen nur helfen kann, ihre Instanzen zu härten.

Einfluss

Wir konnten keine Möglichkeiten finden, dieses Verhalten zu nutzen, um anfällige Instanzen zu übernehmen, ohne auf andere anfällige Dienste angewiesen zu sein.

Es könnte die Ausnutzung anderer Schwachstellen im internen Netzwerk der betroffenen Organisation erleichtern, beispielsweise durch die Verwendung einer der jüngsten Confluence OGNL-Injektionen, der epischen Remote-Code-Ausführung in Jenkins, die von @orange_8361 gefunden wurde , oder einer der anderen von AssetNote dokumentierten Ketten .

Technische Details

Verwendung des anfälligen Konstrukts in der Pingback-Funktion

Pingbacks sind eine Möglichkeit für Blogautoren, benachrichtigt und angezeigt zu werden, wenn andere

„befreundete“ Blogs auf einen bestimmten Artikel verweisen: Sie werden neben Kommentaren angezeigt und können frei akzeptiert oder abgelehnt werden. Unter der Haube müssen Blogs HTTP-Anfragen aneinander senden, um das Vorhandensein von Links zu identifizieren. Auch Besucher können diesen Mechanismus auslösen.

Diese Funktion wurde vielfach kritisiert, da sie es Angreifern ermöglicht, verteilte Denial-of-Service-Angriffe durchzuführen, indem sie böswillig Tausende von Blogs auffordern, auf einem einzelnen Server des Opfers nach Pingbacks zu suchen. Pingbacks sind auf WordPress-Instanzen immer noch standardmäßig aktiviert, da soziale und Community-Funktionen für das persönliche Bloggen wichtig sind. Es wird jedoch nicht erwartet, dass diese Anfragen an andere interne Dienste gesendet werden, die auf demselben Server oder lokalen Netzwerksegment gehostet werden.

Die Pingback-Funktionalität wird auf der XML-RPC-API von WordPress bereitgestellt. Zur Erinnerung: Dies ist ein API-Endpunkt, der XML-Dokumente erwartet, in denen der Client eine aufzurufende Funktion zusammen mit Argumenten auswählen kann.

Eine der implementierten Methoden ist pingback.ping und erwartet die Argumente pagelinkedfrom und pagelinkedto : Das erste ist die Adresse des Artikels, der auf das zweite verweist.

pagelinkedto muss auf einen bestehenden Artikel der lokalen Instanz zeigen, hier http://blog.tld/?p=1 , und pagelinkedfrom auf die externe URL, die einen Link zu pagelinkedto enthalten soll .

Unten sehen Sie, wie eine Anfrage an diesen Endpunkt aussehen würde:

```
POST /xmlrpc.php HTTP/1.1
Host: blog.tld
[...]
```

```
<methodCall>
   <methodName>pingback.ping</methodName>
  <params>
    <param>
      <value><string>http://evil.tld</string></value>
    </param>
    <param>
      <value><string>http://blog.tld/?p=1</string></value>
    </param>
  </params>
</methodCall>
```

Implementierung der URL-Validierung

Die WordPress-Core-Methode wp_http_validate_url() führt einige Überprüfungen der vom Benutzer bereitgestellten URLs durch, um das Missbrauchsrisiko zu verringern. Zum Beispiel:

1. Das Ziel darf keinen Benutzernamen und kein Passwort enthalten;
2. Der Hostname darf folgende Zeichen nicht enthalten: #:?[]
3. Der Domänenname sollte nicht auf eine lokale oder private IP-Adresse wie 127.0.0.1, 192.168.* usw. verweisen.
4. Der Zielport der URL muss entweder 80, 443 oder 8080 sein.

Der dritte Schritt kann das Auflösen von Domänennamen beinhalten, falls sie in der URL vorhanden sind (z. B. http://foo.bar.tld). In diesem Fall wird die IP-Adresse des Remote-Servers ermittelt, indem die URL analysiert **[1]** und später aufgelöst wird **[2]** , bevor sie validiert wird, um nicht öffentliche IP-Bereiche auszuschließen:

src/wp-includes/http.php

```
$parsed_url = parse_url( $url ); // [1]
// [...]
```

```
$ip = gethostbyname( $host );    // [2]
        if ( $ip === $host ) {
           // Error condition for gethostbyname().
                return false;
        }
     // IP validation happens here
}
// [...]
```

Der Validierungscode scheint korrekt implementiert zu sein, und die URL gilt jetzt als vertrauenswürdig. Was passiert als nächstes?

Implementierung des/der HTTP-Client(s)

Zwei HTTP-Clients können Pingback-Anfragen verarbeiten, nachdem sie die URL validiert haben, basierend auf verfügbaren PHP-Funktionen: Requests_Transport_cURL und Requests_Transport_fsockopen . Sie sind beide Teile der Requests- Bibliothek, die unabhängig voneinander unter dem Dach von WordPress entwickelt wurden.

Werfen wir einen Blick auf die Implementierung des letzteren. Wir wissen, dass es die PHP-Streams-API von seinem Namen verwendet. Es arbeitet auf der Transportebene, und der Client muss die HTTP-Anforderung manuell erstellen. Die URL wird erneut mit parse_url() geparst und dann wird ihr *Host* – Teil verwendet, um ein Ziel zu erstellen, das mit der PHP-Streams-API kompatibel ist (z. B. tcp://host:port):

wp-includes/Requests/Transport/fsockopen.php

```
public function request($url, $headers = array(), $data = array(), $options = array()) {
    // [...]
    $url_parts = parse_url($url);
    // [...]
    $host = $url_parts['host'];
    else {
        $remote_socket = 'tcp://' . $host;
```

```
    }
    // [...]
    $remote_socket .= ':' . $url_parts['port'];
```

Weiter entfernt wird dieses Ziel verwendet, um mit stream_socket_client() einen neuen Stream zu erstellen , und die HTTP-Anforderung wird erstellt und dorthin geschrieben:

wp-includes/Requests/Transport/fsockopen.php

```
□□$socket = stream_socket_client($remote_socket, $errno, $errstr,          ceil($options['connect_timeout']), STREAM_CLIENT_CONNECT, $context);
// [...]
$out = sprintf("%s %s HTTP/%.1F\r\n", $options['type'], $path, $options['protocol_version']);
// [...]
if (!isset($case_insensitive_headers['Host'])) {
    $out .= sprintf('Host: %s', $url_parts['host']);
    // [...]
}
// [...]
fwrite($socket, $out);
```

Wie wir sehen können, impliziert dieser Prozess eine andere DNS-Auflösung, sodass stream_socket_client() die IP des Hosts identifizieren kann, um die Pakete zu senden.

Das Verhalten des anderen HTTP-Clients, cURL, ist sehr ähnlich und wird hier nicht behandelt.

Die Schwachstelle

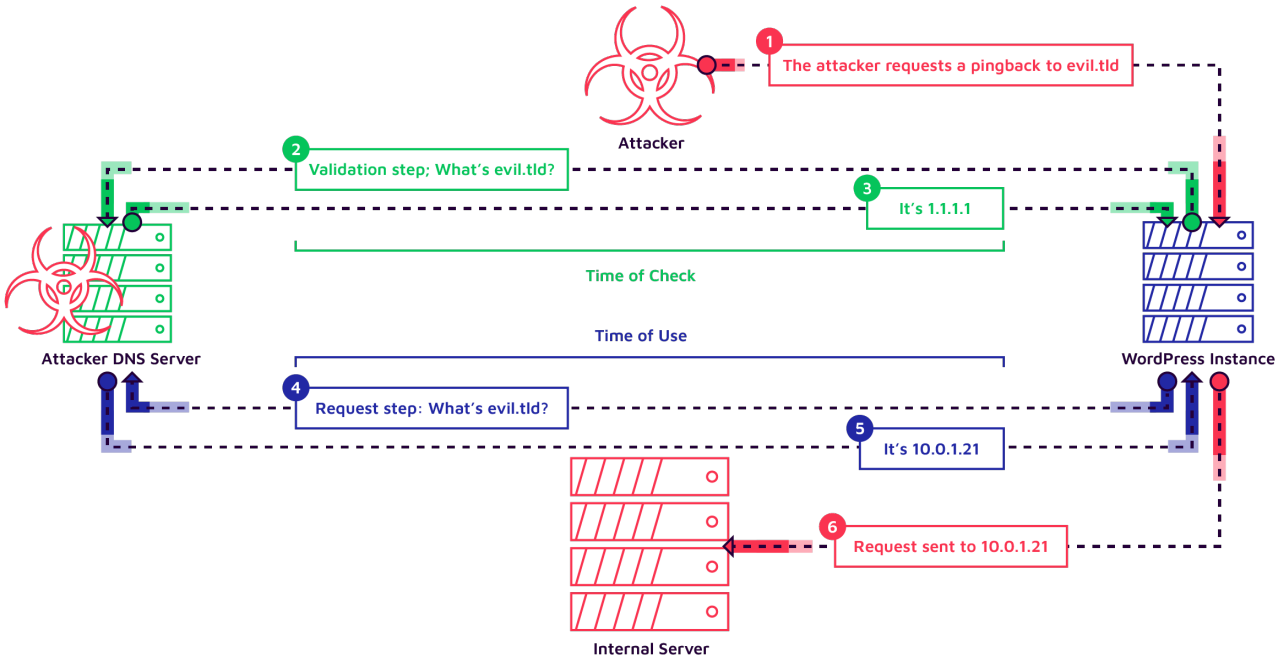
Dieses Konstrukt hat ein Problem: Der HTTP-Client muss die URL erneut analysieren und den Hostnamen erneut auflösen, um seine Anfrage zu senden. **In der Zwischenzeit könnte ein Angreifer die Domain so geändert haben, dass sie auf eine andere Adresse als die zuvor validierte verweist!**

Diese Fehlerklasse wird auch Time-of-Check-Time-of-Use genannt: Eine Ressource wird validiert, kann aber später vor

ihrer effektiven Verwendung geändert werden. Es ist üblich, solche Schwachstellen in Abwehrmaßnahmen gegen serverseitige Anforderungsfälschungen (SSRF) zu finden. Wir haben in unserem Code Security Adventskalender 2021 sogar eine Herausforderung veröffentlicht, die auf diesem anfälligen Codemuster basiert.

https://platform.twitter.com/embed/Tweet.html?creatorScreenName=sonarsource&dnt=false&embedId=twitter-widget-0&features=eyJ0ZndfdGltZWxpbmVfbGlzdCI6eyJidWNrZXQiOlsibGlua3RyLmVlIiwidHIuZWUiLCJ0ZXJyYS5jb20uYnIiLCJ3d3cubGlua3RyLmVlIiwid3d3LnRyLmVlIiwid3d3LnRlcnJhLmNvbS5iciJdLCJ2ZXJzaW9uIjpudWxsfSwidGZ3X2hvcml6b25fdGltZWxpbmVfMTIwMzQiOnsiYnVja2V0IjoidHJlYXRtZW50IiwidmVyc2lvbiI6bnVsbH0sInRmd190d2VldF9lZGl0X2JhY2tlbmQiOnsiYnVja2V0Ijoib24iLCJ2ZXJzaW9uIjpudWxsfSwidGZ3X3JlZnNyY19zZXNzaW9uIjp7ImJ1Y2tldCI6Im9uIiwidmVyc2lvbiI6bnVsbH0sInRmd19zaG93X2J1c2luZXNzX3ZlcmlmaWVkX2JhZGdlIjp7ImJ1Y2tldCI6Im9uIiwidmVyc2lvbiI6bnVsbH0sInRmd19jaGluX3BpbGxzXzE0NzQxIjp7ImJ1Y2tldCI6ImNvbG9yX2ljb25zIiwidmVyc2lvbiI6bnVsbH0sInRmd190d2VldF9yZXN1bHRfbWlncmF0aW9uXzEzOTc5Ijp7ImJ1Y2tldCI6InR3ZWV0X3Jlc3VsdCIsInZlcnNpb24iOm51bGx9LCJ0Zndfc2Vuc2l0aXZlX21lZGlhX2ludGVyc3RpdGlhbF8xMzk2MyI6eyJidWNrZXQiOiJpbnRlcnN0aXRpYWwiLCJ2ZXJzaW9uIjpudWxsfSwidGZ3X2V4cGVyaW1lbnRzX2Nvb2tpZV9leHBpcmF0aW9uIjp7ImJ1Y2tldCI6MTIwOTYwMCwidmVyc2lvbiI6bnVsbH0sInRmd19kdXBsaWNhdGVfc2NyaWJlc190b19zZXR0aW5ncyI6eyJidWNrZXQiOiJvbiIsInZlcnNpb24iOm51bGx9LCJ0ZndfdmlkZW9faGxzX2R5bmFtaWNfbWFuaWZlc3RzXzE1MDgyIjp7ImJ1Y2tldCI6InRydWVfYml0cmF0ZSIsInZlcnNpb24iOm51bGx9LCJ0Zndfc2hvd19ibHVlX3ZlcmlmaWVkX2JhZGdlIjp7ImJ1Y2tldCI6Im9uIiwidmVyc2lvbiI6bnVsbH0sInRmd19zaG93X2dvdl92ZXJpZmllZF9iYWRnZSI6eyJidWNrZXQiOiJvZmYiLCJ2ZXJzaW9uIjpudWxsfSwidGZ3X3Nob3dfYnVzaW5lc3NfYWZmaWxpYXRlX2JhZGdlIjp7ImJ1Y2tldCI6Im9mZiIsInZlcnNpb24iOm51bGx9LCJ0ZndfdHdlZXRfZWRpdF9mcm9udGVuZCI6eyJidWNrZXQiOiJvbiIsInZlcnNpb24iOm51bGx9fQ%3D%3D&frame=false&hideCard=false&hideThread=false&id=1468248939379847168&lang=en&origin=https%3A%2F%2Fblog.sonarsource.com%2F%2Fwordpress-core-unauthenticated-blind-ssrf%2F&sessionId=b21903e53850f875895c48efb872fe3f48f36be0&siteScreenName=blog_SonarSource&theme=light&widgetsVersion=a3525f077c700%3A1667415560940&width=550px

Wie diese aufeinanderfolgenden Schritte aussehen, haben wir im folgenden Diagramm zusammengefasst:



Ausbeutungsszenarien

Wir haben den Code in der Hoffnung geprüft, differenzielle Parser-Fehler zu finden, die es ermöglichen würden, unbeabsichtigte Ports zu erreichen oder POST-Anforderungen ohne Erfolg durchzuführen: Die anfänglichen URL-Validierungsschritte sind restriktiv genug, um ihre Ausnutzung zu verhindern. Wie bereits erwähnt, müssten Angreifer dieses Verhalten mit einer anderen Schwachstelle verketten, um die Sicherheit der angegriffenen Organisation erheblich zu beeinträchtigen.

Patch

Zum Zeitpunkt der Erstellung dieser Veröffentlichung sind uns keine öffentlichen Patches bekannt; Die obigen Details basieren auf einem Zwischenpatch, der uns während des Offenlegungsprozesses mitgeteilt wurde.

Das Beheben solcher Schwachstellen erfordert das Beibehalten der validierten Daten, bis sie zum Ausführen der HTTP-

Anforderung verwendet werden. Es sollte nach dem Validierungsschritt nicht verworfen oder transformiert werden.

Die WordPress-Betreuer folgten diesem Weg, indem sie ein zweites, optionales Argument in wp_http_validate_url() einführten . Dieser Parameter wird als Referenz übergeben und enthält die IP-Adressen, auf denen WordPress die Validierung durchgeführt hat. Der endgültige Code ist etwas ausführlicher, um ältere Versionen von PHP zu berücksichtigen, aber die Hauptidee ist hier.

Als vorübergehende Problemumgehung empfehlen wir Systemadministratoren, den Handler pingback.ping des XMLRPC-Endpunkts zu entfernen. Eine Möglichkeit, dies zu tun, besteht darin, die functions.php des verwendeten Designs zu aktualisieren, um den folgenden Aufruf einzuführen:

```
add_filter('xmlrpc_methods', function($methods) {
  unset($methods['pingback.ping']);
  return $methods;
});
```

Es ist auch möglich, den Zugriff auf xmlrpc.php auf Webserver-Ebene zu blockieren.

Zeitleiste

Datum	Handlung
2022-01-21	Wir übermitteln die Schwachstelle an die Betreuer mit einer 90-tägigen Offenlegungsrichtlinie.
2022-01-21	Unsere Einreichung wird als Duplikat gegen einen Bericht geprüft, der ursprünglich vor (genau) 5 Jahren (2017-01-21) gesendet wurde.
2022-04-11	WordPress beantragt eine Verlängerung unserer 90-tägigen Offenlegungsrichtlinie um 30 Tage, da sie mehr Zeit benötigen, um an Backports zu arbeiten. Sind wir uns einig.

Datum	Handlung
2022-05-23	Maintainer teilen einen Patch für WordPress 5.9.3.
2022-06-01	Wir haben positives Feedback zum Patch gegeben.
2022-07-16	Wir teilen unsere Absicht mit, diese Veröffentlichung am 6. September zu veröffentlichen.
2022-09-01	Abschließende Hinweise zur bevorstehenden Veröffentlichung.
2022-09-06	Dieser Artikel wird 228 Tage nach unserem Bericht und 2054 Tage nach dem ersten Bericht eines anderen Forschers veröffentlicht.

Zusammenfassung

In diesem Artikel haben wir eine blinde SSRF-Schwachstelle beschrieben, die WordPress Core betrifft. Während die Auswirkungen in diesem Fall als gering angesehen werden, handelt es sich um ein weit verbreitetes anfälliges Codemuster, dem wir selbst bei großen Projekten immer wieder begegnen. Wir empfehlen Entwicklern, ihre eigenen Codebasen auf diese Art von Codeschwachstellen zu überprüfen, die sich, wie wir gezeigt haben, sogar in sehr populärem und gut überprüftem Code verstecken können.

Wir möchten den WordPress-Betreuern für ihre Hilfe bei der Lösung dieses Problems danken, auch wenn wir nicht das bestmögliche Ergebnis erzielen konnten.

Verwandte Blog-Beiträge

- WordPress 5.8.3 – Schwachstelle durch Objektinjektion
- WordPress 5.8.2 – Gespeicherte XSS-Schwachstelle
- WordPress 5.7 – XXE-Schwachstelle
- WordPress 5.1 – CSRF zur Remotecodeausführung
- WordPress 5.0.0 – Remote-Code-Ausführung

Simon Scannell und Thomas Chauchefoin Schwachstellenforscher

Wie die EU ihre Digitalstrategie vorantreibt

Im Regulierungsrausch

Nationale Regierungen müssen sich daran gewöhnen: Relevante Gesetze werden zunehmend in Brüssel geschrieben. Gerade in der Digitalpolitik schleudert die Kommission einen Verordnungsvorschlag nach dem anderen heraus, um Versäumnisse aufzuholen und Zukunftstechnologien frühzeitig zu regulieren. Das kl…

Wie die EU ihre Digitalstrategie vorantreibt

Nationale Regierungen müssen sich daran gewöhnen: Relevante Gesetze werden zunehmend in Brüssel geschrieben. Gerade in der Digitalpolitik schleudert die Kommission einen Verordnungsvorschlag nach dem anderen heraus, um Versäumnisse aufzuholen und Zukunftstechnologien frühzeitig zu regulieren. Das klappt manchmal, ist aber auch oft widersprüchlich.

Von Falk Steiner

kompakt

- Die EU zieht im digitalen Bereich immer mehr Kompetenzen an sich und übernimmt auch Aufsichtsfunktionen.
- Insbesondere zu den USA ist die Beziehung kompliziert, weil sich die großen Tech-Konzerne nur ungern an die Regeln der lukrativen europäischen Märkte anpassen.
- Einige Pläne, vor allem der CSAM-Act, schießen deutlich über das Ziel hinaus und werden 2023 für heftige Konflikte zwischen den Mitgliedsstaaten sorgen.

Das dritte Jahrzehnt des 21. Jahrhunderts müsse zur „digitalen Dekade“ werden. Dies hatte EU-Kommissionspräsidentin Ursula von der Leyen in ihrer „Rede zur Lage der Europäischen Union“ im September 2020 angekündigt – und direkt Taten folgen lassen. Bereits ein Jahr später war ein Konzept erkennbar, inklusive neu entwickelter Instrumente, um den digitalen Fortschritt zu messen.

Beispielsweise hat die Kommission den „Index für die digitale Wirtschaft und Gesellschaft“ (DESI) geschaffen, der Fortschritte bei den Zielmarken für 2030 in jedem EU-Mitgliedsstand abbildet und damit Wettbewerb der Staaten untereinander anfacht. In einem jährlichen Bericht über den

„Stand der digitalen Dekade“ bewertet die Kommission außerdem die Fortschritte, beispielsweise bei der Digitalisierung von Verwaltungsakten.

Vor allem aber hat die Kommission, die als einziges EU-Organ Gesetze entwerfen und vorschlagen darf, ein wahres Feuerwerk an neuen Regelwerken fürs Digitale auf die Schiene gesetzt [1]. Einige der Gesetzentwürfe stehen bereits davor, umgesetzt zu werden, bei anderen suchen Kommission, EU-Parlament und Europäischer Rat noch Kompromisse. Und die Lust auf mehr Regulierung ist in Brüssel noch lange nicht verflogen – auch fragwürdige Ideen sind auf dem Weg.

Der Brüssel-Effekt

Den Startschuss für die digitale Dekade gab die EU eigentlich schon im Mai 2018: Damals wurde die EU-Datenschutz-Grundverordnung (DSGVO) wirksam. Sie setzt bis heute die Grenzen dafür, wie Unternehmen und Behörden Daten von EU-Bürgern nutzen dürfen – auch für alle nachfolgenden Gesetze. Die EU-Kommission hatte darauf gesetzt, mit der DSGVO nationale Datenschutzgesetze abzulösen und einheitliche Regelungen für den gesamten Binnenmarkt zu schaffen. Dies gilt mittlerweile als Erfolgsmodell, weshalb viele neue Vorhaben als für alle 27 Mitgliedsstaaten verbindliche Verordnungen daherkommen statt als schwächere Richtlinien.

Denn die DSGVO hat gezeigt: Als Absatzmarkt ist die EU mit ihren fast 450 Millionen kaufkräftigen Einwohnern für viele Unternehmen zu wichtig, um sie zu ignorieren – unter anderem auch für Amazon, Apple, Meta, Google und die anderen großen Akteure. Wer in Europa Profite machen will, muss sich ihren Regeln unterwerfen. Ob bei Anschlussbuchsen, Ladegeräten, im Daten-, Wettbewerbs- und Kartellrecht, bei der Plattformgesetzgebung, IT-Sicherheit oder KI-Regulierung: Nationale Regeln sind an vielen Stellen mittlerweile schlicht zu unbedeutend.

Dieser sogenannte Brüssel-Effekt führt dazu, dass Europa immer mehr Kompetenzen an sich zieht – und das mit Unterstützung der Mitgliedstaaten. Die meisten davon haben begriffen, dass sie alleinstehend wenig ausrichten können. Mit der Kraft der EU lockt eine mächtige Verhandlungsposition.

Komplizierte Beziehung

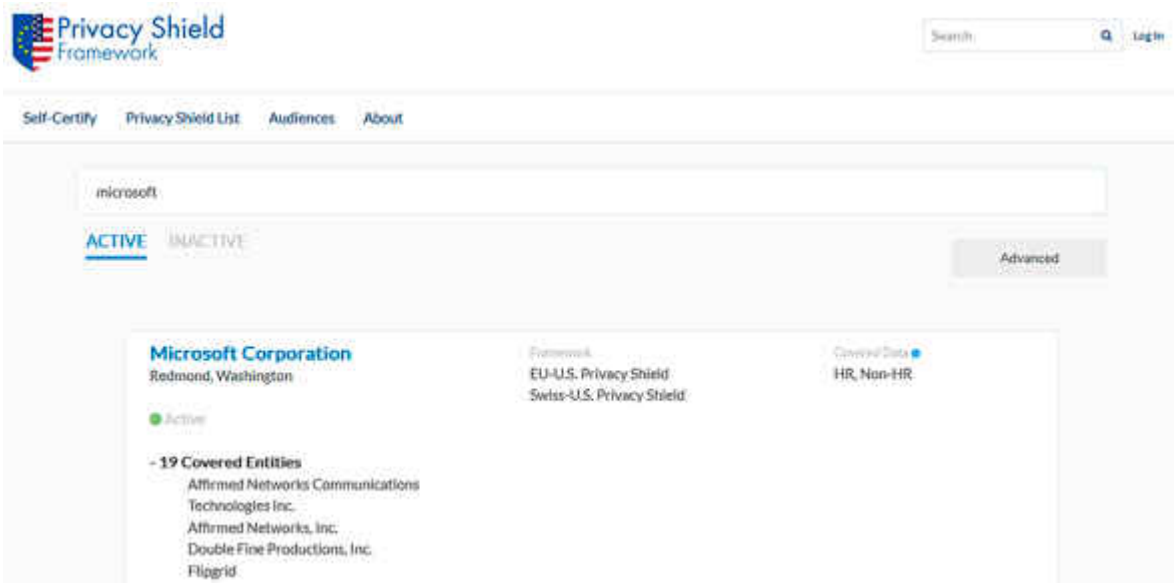
Seit dem Amtsantritt Joe Bidens in den USA und dem Angriff Russlands auf die Ukraine sind weitere Einflüsse auf künftige Regulierung maßgeblich geworden. Vor allem eine Frage treibt Politiker in Brüssel um: Auf wen wird man sich in Zukunft verlassen können? Ihre naheliegende Antwort: Auf als stabil erachtete Demokratien überall in der Welt. Seit Monaten führen EU-Politiker auf vielen Ebenen Gespräche und loten aus, wie sich „die Guten“ dieser Welt untereinander besser vernetzen können, um resilienter gegen böswillige Akteure zu werden.

Handelsabkommen wie CETA mit Kanada, das lange auf Eis lag, sollen nun doch kommen. Vorteilhaft: Auch in den USA gibt es durchaus Lust auf mehr Regulierung. Das ist nicht zuletzt der wachsenden Macht chinesischer Staatsunternehmen, aber auch der einheimischen Kritik am Gebaren einiger US-Konzerne geschuldet.

Aber nicht nur mit Investitionen, auch regulatorisch versucht die EU den Schulterschluss mit den USA. Der eigentliche Lackmustest für die neu belebten transatlantischen Beziehungen steht noch bevor: Im Frühjahr 2023 wird die EU-Kommission über den Transfer personenbezogener Daten in die USA entscheiden. Der erwartete Angemessenheitsbeschluss als Nachfolgeregelung des gescheiterten Privacy Shields ist elementar für Wirtschaft und Nutzer auf beiden Seiten des Atlantiks. Denn wenn keine neue, sichere Rechtsgrundlage geschaffen wird, dürfen viele US-Unternehmen nicht mehr mit den persönlichen Daten von EU-Bürgern arbeiten.

Salesforce, Amazon, Google, Apple, Meta und Microsoft könnten

für EU-Daten zur Tabuzone werden. Meta etwa warnt immer wieder davor, dass möglicherweise das EU-Geschäft eingestellt werden müsste – ein Milliardenmarkt würde dem Konzern verloren gehen. Damit das nicht passiert, müssten die USA die Sicherheit von EU-Daten auch gegenüber den US-Nachrichtendiensten verbessern und die Hürden für Zugriffe höher legen. Bislang liegt aber lediglich ein Vorschlag seitens der US-Regierung vor, der bessere Beschwerdemöglichkeiten vorsieht. Dafür hat US-Präsident Biden Anfang Oktober ein Dekret unterzeichnet, und die EU-Kommission muss nun entscheiden, ob das ausreicht [2].



Auf Eis: Viele US-Konzerne wie Microsoft haben sich zwar selbst für den EU-US-Datentransfer zertifiziert, dürfen sich aber derzeit nicht darauf berufen.

Parallel dazu ist die EU bemüht, sich US-Unternehmen als Spielfeld für die sogenannten Zukunftsmärkte im IT-Sektor zu präsentieren. Das ist kein leichtes Unterfangen, denn gerade hier reguliert sie exzessiv herum: Um die KI-Verordnung (AI-Act), die zumindest besonders kritische KI-Anwendungen mit strikteren Regeln versehen soll, wird seit dem Amtsantritt Ursula von der Leyens 2020 gerungen. Bereits seit Frühjahr 2021 liegen die Vorschläge der Kommission auf dem Tisch. Es geht nur zäh voran: Das Parlament und die Mitgliedstaaten suchen nach Lösungen, während KI-Anwendungen in immer mehr Endgeräte und Anwendungen Einzug halten.

Die strittige Haftung für automatisierte Entscheidungen hat man nun aus der Verordnung herausgenommen: Für KI im engeren Sinne und für den Einsatz im Rahmen marktgängiger Produkte und Dienstleistungen hat die Kommission Ende September neue Regelungsvorschläge unterbreitet. Sie sollen gewährleisten, dass von KI-Entscheidungen unrechtmäßig Benachteiligte ihre Betroffenheit auch nachweisen können. Bei der begründeten Annahme, dass ein Unternehmen nicht alle Regeln eingehalten hat, soll in einigen Fällen eine „Vermutungsregel“ zugunsten der Betroffenen greifen – für Anwälte könnte da ein weiteres interessantes Geschäftsfeld entstehen.

Alles für die Kinder?

Wo sogenannte KI nach dem Willen der Kommission entgegen aller Bedenken intensiv zum Einsatz kommen soll, ist beim Kampf gegen Missbrauchsdarstellungen von Kindern im Internet. Als Sammelbegriff für dieses Material hat sich auch hierzulande das US-amerikanische Akronym CSAM (Child Sexual Abuse Material) etabliert. Ein im Mai 2022 vorgestellter Gesetzentwurf wird deshalb auch kurz CSAM-Verordnung genannt. Dieses Vorhaben der EU-Innenkommissarin steht inhaltlich stark in der Kritik: Mit dem Gesetz könnten Plattformanbieter wie Apple, Meta, Microsoft und Google dazu verpflichtet werden, automatisiert nach CSAM-Inhalten zu fahnden und mutmaßliche Treffer an ein europäisches Zentrum zur Bekämpfung derartiger Inhalte zu melden. Bislang tun das einige auf Grundlage einer befristeten Erlaubnis bereits heute. Microsoft etwa durchforstet seinen Cloud-Speicher OneDrive auf CSAM-Material hin und sperrt deshalb bisweilen unberechtigt Nutzerkonten [3].

Bürgerrechtler stellen denn auch immer wieder infrage, dass die KI-gestützten Filter CSAM-Abbildungen ausreichend zuverlässig erkennen. Sie sehen die Gefahr von Falschverdächtigungen für größer an als den Nutzen, zumal die Pflicht nach den Plänen der Kommission auch Anbieter

verschlüsselter Chats träfe – was zu einem heftigen Eingriff ins Grundrecht auf vertrauliche Kommunikation führen würde [4]. Zudem könnten Strafverfolgungsbehörden laut Kommissionsvorschlag Zugangsanbieter dazu verpflichten, Sperren gegen Websites einzurichten, die nicht genug gegen derartige Inhalte unternehmen. Da der Vorschlag technikneutral formuliert ist, bezieht er sich nicht nur auf klassische Webseiten: auch Betreiber anderer digitaler Kommunikationswege, etwa Tor-Hoster, könnten davon betroffen sein.

Gegenwind aus Deutschland: Bürgerrechtsorganisationen sammeln gemeinsam auf der Petitionsplattform Campact Unterschriften gegen die geplante CSAM-Verordnung der EU-Kommission.
Das Vorhaben gilt insbesondere in Deutschland als politisch heißes Eisen. In der Bundesregierung hat sich Bundesinnenministerin Nancy Faeser (SPD) grundsätzlich dafür ausgesprochen, die FDP-geführten Digital- und Justizministerien dagegen. Auch im Europaparlament gibt es Widerstand vor allem aus Reihen von FDP, Grünen und Piraten gegen die dort unter dem Begriff Chatkontrolle laufenden Pläne der Kommission. Ob das Parlament den Plan im Gesetzgebungsprozess stoppen oder doch nur abmildern kann, wird sich frühestens 2023 entscheiden.

Sicherheit vor allzu wilden Politikerideen lässt sich nicht verordnen – sehr wohl aber mehr Cybersicherheit für Endgeräte und kritische Infrastruktur: Für beide Themen liegen

Vorschläge auf dem Tisch. Die überarbeitete Netzwerk- und Informationssicherheits-Richtlinie NIS ist bereits unter Dach und Fach – die Mitgliedstaaten müssen sie nun in nationales Recht umsetzen. Für Deutschland bringt sie vergleichsweise wenig Änderungen mit sich, dennoch werden 2023 einige Änderungen am IT-Sicherheitsgesetz fällig, um dem genauen Wortlaut der Revision zu entsprechen.

Anders sieht es mit dem Cyber Resilience Act (CRA) genannten Kommissionsvorschlag vom Herbst 2022 aus – es stehen harte Verhandlungen zwischen Kommission, Parlament und Rat an. Unter anderem geht es um Anforderungen an netzwerkfähige Endgeräte, die nicht von Spezialregeln (etwa für kritische Infrastruktur) umfasst sind. Die Kommission begreift ihren Vorschlag als Antwort etwa auf die Erfahrungen mit dem Mirai-Botnetz, das eine große Zahl nicht gesicherter Webcams für DDoS-Attacken missbrauchte. Mit dem CRA sollen Anbieter von derlei Produkten von Betroffenen in die Pflicht genommen werden können. Halten sie sich nicht an definierte Sicherheitskriterien, haften sie für Schäden – so zumindest der Plan der EU, der im kommenden Jahr verabschiedet werden soll.

Notdürftige Reparaturen

Die Eile, mit der die Kommission einige der Gesetzeswerke derzeit unkoordiniert durch die Institutionen peitscht, führt zu jeder Menge neuer Probleme. Zum Beispiel die Cookie-Problematik: Sie ist bis heute auf EU-Ebene nicht abschließend gelöst – ein echtes Ärgernis für alle Beteiligten, sowohl Unternehmen als auch Verbraucher. Die Kommission hatte geplant, dass die sogenannte E-Privacy-Verordnung eindeutige Regeln vorgibt. Doch die steckt seit über vier Jahren im Prozess fest und wurde von der DSGVO überholt, aus der nun Datenschutzbehörden notgedrungen Regeln ableiten müssen, die nicht drinstehen. Die Gemengelage aus DSGVO und noch gültiger, überalterter E-Privacy-Richtlinie lässt zu viel Interpretationspielraum – eine umfassende Lösung gibt es

bislang nicht, nur notdürftige Reparaturen [5].

Gegen irreführende Techniken bei Einwilligungsbannern („Dark Patterns“) hat die EU zuletzt auf Drängen der Europaparlamentarier in den ab April 2024 wirksamen Digital Services Act (DSA) eine Regelung aufgenommen. Das deutsche Digitalministerium erarbeitet parallel auf Grundlage des deutschen Telemedien-Teledienste-Datenschutzgesetzes (TTDSG) eine Regelung für die zentralisierte Einwilligungsverwaltung. Von der erhofft sich die Ampelregierung, einen großen Knoten in der Debatte um die E-Privacy-Verordnung vorbildhaft durchschlagen zu können, sodass sie irgendwann doch noch kommen kann – mit einem halben Jahrzehnt Verspätung [6].

Viele der zuletzt verabschiedeten oder derzeit im Beratungsprozess steckenden Gesetzgebungen zeigen aber auch, dass die EU dazulernt: Während mit der DSGVO noch versucht wurde, starke und unabhängige Aufsichtsbehörden in den Mitgliedstaaten zu schaffen, plant die Kommission neuere Vorschläge deutlich zentralistischer – und das teils auf ausdrücklichen Wunsch der EU-Staaten, vertreten durch den Europäischen Rat. Denn wenn im Binnenmarkt eine der Behörden nicht mitspielt, entsteht ein exekutiver Flaschenhals, wie die irische Datenschutz-Aufsichtsbehörde DPC mit ihrer laxen Verfolgung von Datenschutzverstößen immer wieder belegt.

Mit dem DSA und dem Digital Markets Act (DMA) hat die EU nun bereits zwei Gesetze verabschiedet, bei denen die Kommission im kommenden Jahr das Aufsichtsregime zusammensetzt. Geplant ist ein Zusammenspiel nationaler und europäischer Aufsichtsbehörden. Für die extrem großen Player am Markt wird die EU-Kommission selbst als Aufsicht fungieren.

Bei der Plattformaufsicht im DSA muss sich insbesondere Deutschland umsortieren. Das umfangreiche Gesetzeswerk verändert unter anderem den Mechanismus, wann und wie Plattformbetreiber im Netz bei rechtswidrigen Inhalten eingreifen müssen. Was in Deutschland bislang über das

Netzwerkdurchsetzungsgesetz (NetzDG) geregelt war, wird ab 2024 vom DSA überschrieben. Und der geht in Teilen sogar über das hinaus, was das umstrittene NetzDG vorgibt. Damit werden im kommenden Jahr Änderungen am deutschen Recht nötig, die auch die Nutzer von sozialen Medien betreffen.

Zankapfel Traffic-Kosten

Überrascht waren im Mai 2022 Beobachter und Regulierungsbehörden, als Kommissionsvizepräsidentin Margrete Vestager und der Binnenmarktkommissar Thierry Breton einen neuen Vorstoß unternahmen, einige Anbieter im Netz künftig mehr für die Infrastruktur zahlen zu lassen. Kern der Debatte: Sehr wenige Akteure verursachen einen Großteil des Datenverkehrs im Netz – tragen in der Wahrnehmung der ausbauenden Telekommunikationsunternehmen und der EU-Kommission aber zu wenig der entstehenden Kosten. Insbesondere geht es um den Breitbandausbau in der Fläche, den viele Mitgliedstaaten teuer subventionieren.

Wer soll das bezahlen? Nach Wünschen zweier EU-Kommissare sollen Streaminganbieter wie Netflix an den Kosten für den Glasfaserausbau in der Fläche beteiligt werden. *Bild: Deutsche*

Telekom
Zwei unvereinbare Positionen prallen aufeinander: Die Anbieter von Streamingdiensten wie Netflix oder Amazon, deren hochauflösende Videos statistisch große Teile des Verkehrs verursachen, argumentieren damit, dass erst ihre Angebote teure Netzzugänge und den weiteren Ausbau attraktiv machen würden. Einige der Telekommunikationsanbieter wiederum argumentieren, dass diese ohne die Breitbandzugänge keine Umsätze generieren könnten.

Derzeit überarbeitet die EU die Richtlinie zur Reduzierung der Breitbandkosten. Im Laufe des Jahres 2022 rückten Vestager und Breton von ihrem Plan zwar nicht ab – von einem schnellen Abschluss der Revision ist seit dem Herbst aber nicht mehr die Rede. Stattdessen soll nun in einem geregelten Prozess ermittelt werden, ob tatsächlich finanzielle Ungleichgewichte bestehen und ob sich daraus Handlungsbedarf ergibt. Dieses Vorgehen hatten auch die nationalen Regulierungsbehörden verlangt.

Eine breite Koalition aus Mitgliedstaaten, Verbraucherschützern und Europaparlamentariern hatte davor gewarnt, mit dieser Debatte ein altes Fass wieder aufzumachen: Sollten nicht doch einzelne Dienste gegen Bezahlung bevorzugt werden? Dies würde einen Eingriff in die eigentlich garantierte Netzneutralität bedeuten. Danach sieht es politisch derzeit zumindest nicht aus, doch ein Streit im kommenden Jahr scheint vorprogrammiert.

Bilanz

Im Frühjahr 2024 wählen die EU-Bürger ihr Parlament neu. Offen ist, ob die Von-der-Leyen-Kommission danach die „Digitale Dekade“ weiter umsetzen darf. Einen großen Teil der EU-Digitalstrategie hat sie tatsächlich bereits 2022 auf den Weg gebracht – doch viele der Puzzlestücke sind entweder noch in Arbeit oder werden bereits von neueren Entwicklungen überrollt.

Bei einigen Gesetzgebungsvorhaben ist unklar, ob sie tatsächlich den gewünschten, großen Unterschied machen können. Zugleich lauern auch in den Brüsseler Schubladen der Kommissare immer wieder Ideen, die nicht unbedingt von tieferem Verständnis für die digitalpolitischen Debatten der vergangenen Jahrzehnte zeugen. Und je stärker der außenpolitische Druck wird, desto größer ist die Gefahr, dass auch sicherheitspolitische Ideen wie die Vorratsdatenspeicherung, automatische Inhaltsfilterungen und Websperren in Brüssel Anklang finden.

Bislang ist die Bilanz der aktuellen EU-Kommission durchwachsen. Während sie mit ihrer KI-Gesetzgebung und im Datenrecht vor vielen anderen Initiativen in der Welt liegt und Standards setzt, bei der IT-Sicherheit endlich auch wenig smarte Endgeräte und deren Hersteller in den Blick nimmt, droht in anderen Bereichen Chaos: Neue Regeln allein machen die digitale Welt noch kein bisschen besser. *(hob@ct.de)*

1. Literatur

2. Joerg Heidrich, Europäisches Trommelfeuer, Wie die EU den Umgang mit Daten revolutionieren will, c’t 18/2022, S. 168
3. Holger Bleich, Privacy Shield 2.0, Neues EU-US-Datentransfer-Abkommen nimmt erste Hürde, c’t 23/2022, S. 32
4. Greta Friedrich, Ein Foto – und alles ist weg, Microsoft sperrt Kunden unangekündigt für immer aus, c’t 24/2022, S. 104
5. Holger Bleich, Massenüberwachung durch die Hintertür, Wie ein EU-Kinderschutzgesetz die Presse- und Meinungsfreiheit massiv einschränken könnte, c’t 13/2022, S. 144
6. Holger Bleich, Löcher stopfen per Verordnung, Die bizarre Tracking-Regulierung in Deutschland, c’t 16/2022, S. 34
7. Holger Bleich, Cookie-Banner adieu?, Eine

Rechtsverordnung soll Cookie-Abfragen eindämmen, c’t 20/2022, S. 38

Mehr Vielfalt, schnell wachsende Neulinge: das Social-Media-Jahr 2022

Die Macht der Netzwerke

TikTok wächst schneller als die Konkurrenz und war im vergangenen Jahr stilprägend auch für andere Social-Media-Dienste. Facebook wird immer unwichtiger, dafür holen andere Dienste auf. Elon Musk kauft Twitter. Und nicht nur bei den Unruhen in Iran und beim Ukraine-Krieg spielen die Online-Netzwerke…

TikTok wächst schneller als die Konkurrenz und war im

vergangenen Jahr stilprägend auch für andere Social-Media-Dienste. Facebook wird immer unwichtiger, dafür holen andere Dienste auf. Elon Musk kauft Twitter. Und nicht nur bei den Unruhen in Iran und beim Ukraine-Krieg spielen die Online-Netzwerke eine wichtige Rolle. Der Rückblick auf ein turbulentes Jahr bei den sozialen Medien.

Von Jo Bager und Greta Friedrich

kompakt

- Der Kurzvideodienst TikTok ist so erfolgreich, dass andere Anbieter ihn kopieren; mit BeReal wächst ein neuer Social-Media-Dienst heran.
- Elon Musk hat Twitter übernommen, die Hälfte der Belegschaft entlassen, scheint aber kein Erfolgsrezept für den Kurznachrichtendienst zu haben.
- Soziale Medien sind gerade in Autokratien ein wichtiger Kommunikationskanal für Oppositionelle, etwa in Iran oder in Russland.

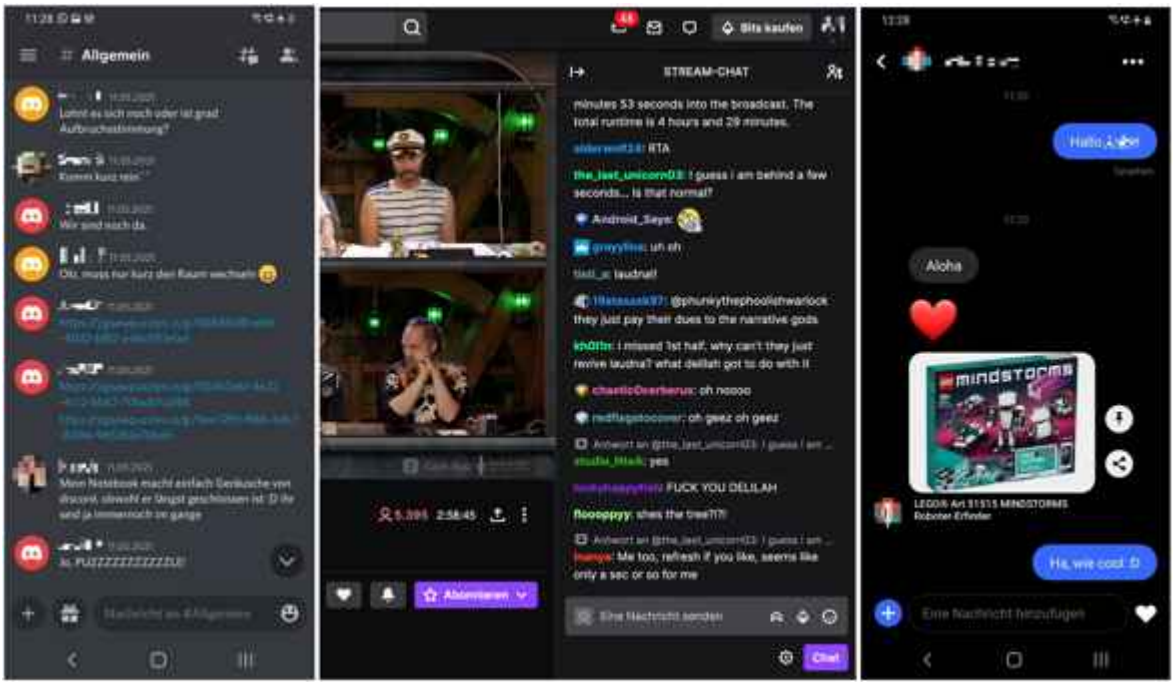
Lange Zeit war Meta verwöhnt, was die Gunst seiner Nutzerschaft anging. Doch in diesem Jahr zeigte sich, dass der Kurzvideodienst TikTok immer beliebter wird, gerade bei den jüngeren Zielgruppen. Das belegt die repräsentative Jugend-Digitalstudie der Postbank. Laut der Studie schauten im Mai und Juni 2022 schon 63 Prozent der Jugendlichen regelmäßig Videos bei TikTok oder luden dort eigene Clips hoch – noch Anfang 2020 war nur ein Viertel der Jugendlichen auf der Plattform aktiv gewesen.

Facebook dagegen verliert gerade für jüngere Menschen immer mehr an Bedeutung. In der Postbank-Studie kam das soziale Netzwerk nur noch auf Platz zehn der meistgenutzten Netzwerke, nur vier Prozentpunkte vor Telegram. Die Meta-Plattformen WhatsApp und Instagram gehören immer noch zu den meistgenutzten Plattformen bei den 16- bis 18-Jährigen in

Deutschland, doch TikToks Beliebtheit wächst schneller als die der anderen Social-Media-Plattformen. Facebook hat auch daran zu knapsen, dass Apple sein Tracking von Werbeanzeigen geändert hat. Meta würden daher Milliarden an Werbeeinnahmen entgehen. Die Folge: gesenkte Wachstumsprognosen und 11.000 Entlassungen bei der Facebook-Mutter.

Kleine Dienste gewinnen

Während dem einstigen Marktführer die Puste ausgeht, legten laut der Postbank-Studie einige Social-Media-Dienste aus der zweiten Reihe im Jahr 2022 teils kräftig zu. Die Chat-Plattform Discord nutzten etwa 35 Prozent der Jugendlichen in Deutschland – sechs Prozentpunkte mehr im Vergleich zu 2020. Das Live-Streaming-Videoportal Twitch, in dem man während einer Übertragung chatten kann, kam auf 24 Prozent und legte um einen Prozentpunkt zu. Auch Twitter gewann junge Nutzer hinzu, holte ebenfalls sechs Prozentpunkte auf und kam auf 23 Prozent. Die Foto-Community Pinterest nutzten 28 Prozent der Jugendlichen, fünf Prozentpunkte mehr als zuvor.



Kleinere Dienste wie Discord, Twitch oder Pinterest (von links) werden bei der jüngeren Zielgruppe immer beliebter. *Discord; Twitch; Pinterest*

TikTok für alles – alle wie TikTok

TikTok aber scheint der Dienst der Stunde zu sein. Gerade die Jüngeren nutzen die Kurzvideoplattform nicht zur bloßen Unterhaltung, sondern auch als Suchmaschine. Das musste sogar Google-Manager Prabhakar Raghavan im Juli zugeben: Ihm zufolge würden beispielsweise 40 Prozent der jungen Menschen auf der Suche nach einem Restaurant nicht Google Maps oder die Google Suche, sondern TikTok oder auch Instagram öffnen. Seine Aussagen beruhen auf internen Studien von Google, darunter eine Umfrage unter Nutzern in den USA im Alter von 18 bis 24 Jahren.

TikToks Erfolg führt dazu, dass die etablierten Plattformen wie Facebook, Instagram aber auch YouTube gern auch so sein wollen: Sie versuchen, den Dienst zu kopieren, und hoffen offenbar, auf diese Weise Nutzer von TikTok zurückzuholen. Augenfällig sind die kurzen Videos, die in immer mehr sozialen Netzwerken aufploppen. Meta setzt Reels in Facebook und Instagram ein, also kurze Video-Endlosschleifen. Und auch YouTube hat einen Bereich „YouTube Shorts“ mit ebensolchen Filmchen. Ab Anfang 2023 sollen Kreative mit den Schnipseln sogar Geld verdienen können, YouTube will sein Monetarisierungssystem dafür öffnen.

Viel Kritik erntete im Juli die überarbeitete Facebook-App. Dort gibt es nun einen „Home Tab“, der gleichsam die Startseite der App ist. Dort sehen Nutzer keine Inhalte befreundeter Menschen mehr, sondern von einem Algorithmus zusammengestellte Posts, darunter viele Reels. Um die gewohnten Posts von Freunden, Gruppen und Seiten zu sehen, muss man in den „Feeds-Tab“ wechseln.

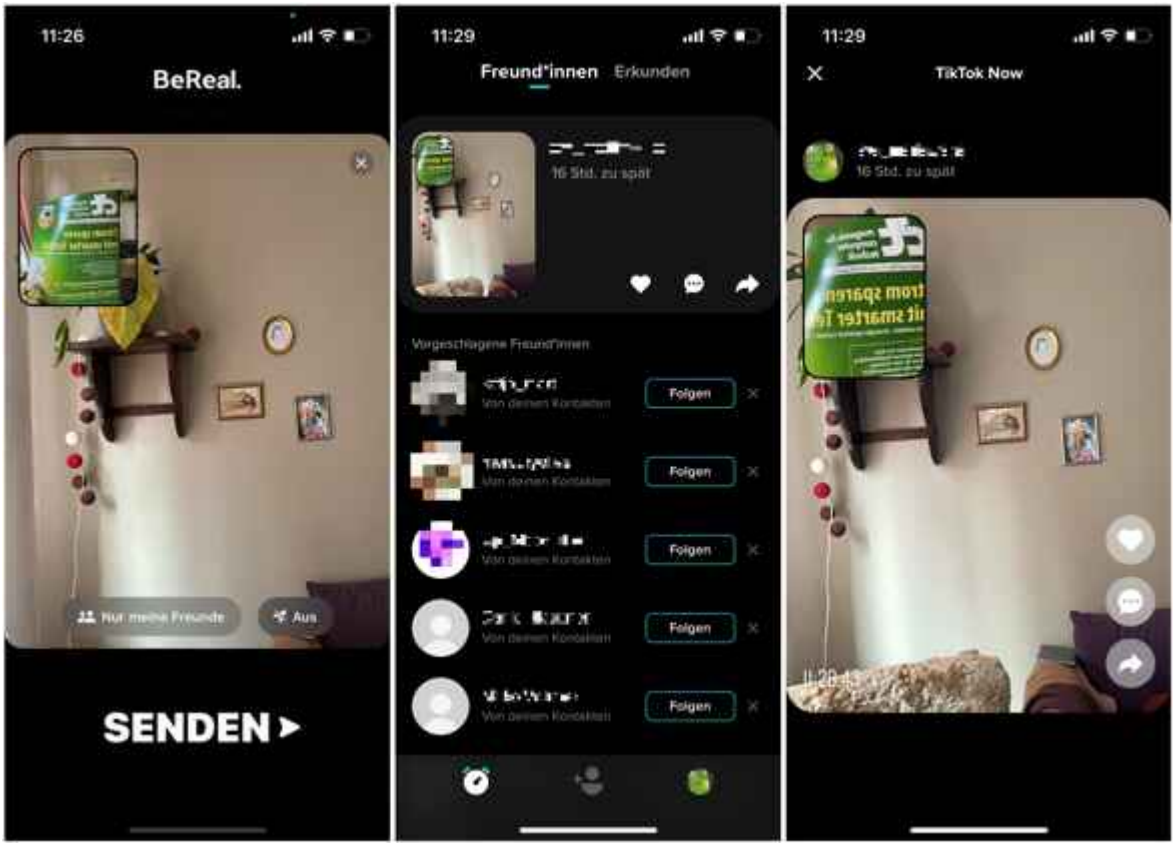
Auch Instagram integrierte im Juli seine Reels in den Newsfeed – zuvor hatten diese sich in einem eigenen Tab versteckt. Doch gegen die Neuerung protestierten viele Instagrammer, vor allem Fotokünstler, die um die Sichtbarkeit ihrer Werke im Newsfeed fürchteten. Ihre Petition „Make Instagram Instagram again“,

die auch die Top-Influencerin Kylie Jenner unterstützte, war erfolgreich: Instagram-Chef Adam Mosseri erklärte, dass die Neuerungen vorerst zurückgenommen würden.

Der kommende Star: BeReal

Doch auch TikTok selbst guckt sich Funktionen bei der erfolgreichen Konkurrenz ab. So hat der Dienst kürzlich die Funktion „TikTok Now“ eingeführt – offensichtlich eine Kopie der französischen App BeReal. Diese App gibt es seit Ende 2019, doch besonders im vergangenen Jahr stiegen ihre Downloadzahlen deutlich an. Vor allem die Generation Z scheint die App zu mögen, also die zwischen 1997 und 2012 Geborenen. In Deutschland, Österreich und der Schweiz testet TikTok die neue „Now“-Funktion derzeit, es gibt sie auch als separate App.

Genau wie BeReal setzt TikTok Now auf Authentizität und Spontaneität. Täglich schickt die Funktion ihren Nutzern eine Push-Nachricht, die diese auffordert, genau jetzt ein Foto oder Kurzvideo aufzunehmen – mit Front- und Rückkamera zugleich. So soll ein Eindruck entstehen, was die jeweilige Person gerade tut. Die Besonderheit: Man soll nach der Push-Nachricht keine Zeit haben, seine Umgebung und sich selbst möglichst perfekt herzurichten. Stattdessen soll so die ungefilterte Wirklichkeit gezeigt werden.



Auch TikTok guckt bei der Konkurrenz ab: Links das Original, die App BeReal in der Mitte und rechts der Klon TikTok Now. *Bild: BeReal; TikTok*

Musk krempelt Twitter um

Bei Twitter war das vergangene Jahr geprägt durch einen längeren Hickhack um die Übernahme durch Elon Musk. Musk war bereits vor 2022 ein scharfer Kritiker der Plattform, der er unter anderem die bis heute andauernde Verbannung von Donald Trump ankreidete.

Im April hatte der Milliardär dem Kurznachrichtendienst ein Übernahmeangebot gemacht. Als künftiger Besitzer wollte er die Plattform „wieder mehr für Free Speech“ öffnen. 44 Milliarden US-Dollar hat er dafür zusammengekratzt, davon etliche Milliarden bei anderen Investoren. Twitter versuchte zunächst, den Kauf zu verhindern, gab dann jedoch nach und beschloss eine Übernahmevereinbarung mit Musk.

Elon Musk unterbreitete Twitter ein Übernahmeangebot – und wies natürlich per Tweet darauf hin. *Bild: Twitter/elonmusk*

Im Juli kündigte Musk den Vertrag allerdings wieder auf. Angeblich habe Twitter mehrere Klauseln nicht eingehalten – darunter die Auskunft zur Anzahl der Bot- und Spam-Konten. Twitter verklagte daraufhin den Milliardär: Er sollte die Übernahme abschließen oder eine Entschädigung von einer Milliarde US-Dollar zahlen. Es folgte eine monatelange juristische Auseinandersetzung.

In diese Querelen spielten die Sicherheitsprobleme des Dienstes herein, die der ehemalige Sicherheitschef des US-Konzerns, Peiter Zatko, im August öffentlich gemacht hat. Die IT-Sicherheit von Twitter habe bei seinem Dienstantritt 2020 mehr als ein Jahrzehnt hinter den Branchenstandards gelegen, sagte er im September bei einer Anhörung vor dem US-Senat.

Am 28. Oktober twitterte Musk dann „the bird is freed" und zog als neuer Chef in die Firmenzentrale ein. Dort feuerte er in den ersten Tagen das Topmanagement, den Verwaltungsrat und entließ die Hälfte der Belegschaft – 3700 Mitarbeiter. Der Rest wurde dazu verdonnert, im Büro zu arbeiten – bisher war ihnen erlaubt, im Home Office zu bleiben. Später wurden dann auch die Verträge mit externen Mitarbeitern gekündigt, darunter Content-Moderatoren. Beobachter gehen davon aus, dass die massiven Einschnitte früher oder später zu technischen

Problemen führen.

Musk scheint kein brauchbares Konzept zu haben, um neue Erlösquellen zu erschließen. Er versuchte, den blauen Haken für verifizierte Accounts mit einer monatlichen Gebühr zu Geld zu machen, gab diesen Versuch aber schon nach einem Tag wieder auf. Derweil haben sich viele Werbekunden nach Musks Übernahme von Twitter zurückgezogen.

Die rechten Alternativen

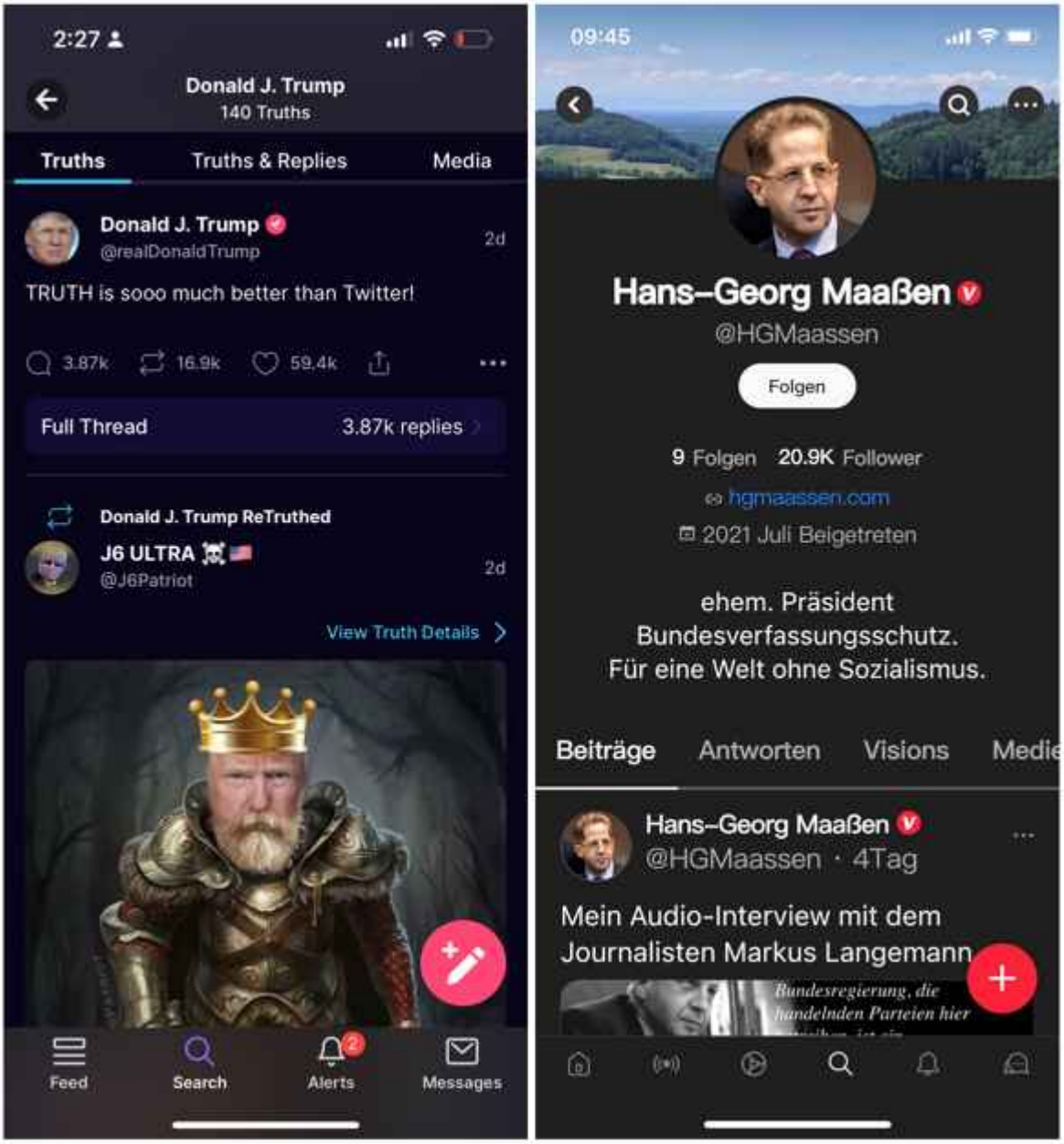
Für die Entwicklung seines Twitter-Klons „Truth Social“ hatte Trump im vergangenen Jahr eigens das Unternehmen „Trump Media & Technology Group“ (TMTG) gegründet. Bis Ende März sollte die Plattform mit allen Funktionen am Start sein. Doch im Herbst 2022 existiert nach wie vor nur eine rudimentäre App für iPhones – Android-Nutzer bleiben bislang außen vor.

Inzwischen droht auch die Finanzierung endgültig zu scheitern: Eigentlich sollte Truth Social über das Börsenvehikel Digital World Acquisition Corp (DWAC) an die Börse gebracht werden, doch das klappte hinten und vorne nicht. Weil Fristen ausgelaufen sind, sprangen jüngst reihenweise Investoren ab, und der Börsenwert von DWAC schwindet außerdem. Trumps groß angekündigte Plattform, die nach seinen markigen Worten „gegen die Tyrannen von Big Tech““ angetreten war, führt ein kümmerliches Dasein mit wenigen Millionen Nutzern.

Alternativen bietet der Markt reichlich, etwa die Netzwerke Parler, Gettr oder Gap. Sie alle laufen in den USA unter dem Begriff „Alt-tech“. Er beschreibt Social-Media-Plattformen und andere Internetdienste, die in der Alt-Right-Bewegung, der extremen Rechten und anderen extremen Gruppierungen populär geworden sind. Bislang erreicht keine von ihnen eine kritische Masse von Nutzern, die sie es mit Twitter aufnehmen lassen könnte.

Gettr etwa spricht von sechs Millionen Nutzern. In einer

Analyse hat das Institute for Strategic Dialogue (ISD) die Aktivitäten im deutschsprachigen Gettr untersucht und kam zu dem Ergebnis, dass „die tatsächliche Anzahl der Follower auf Gettr wesentlich geringer zu sein scheint als auf der Plattform dargestellt, weshalb die tatsächliche Reichweite dieser Profile deutlich geringer ist als auf Twitter“. Viele Akteure nutzen demnach Gettr lediglich als Backup für ihre Twitter- oder Telegram-Profile.



Netzwerke wie Truth Social (Screenshot links) und Gettr können es bisher nicht mit Twitter aufnehmen, sie haben viel weniger Nutzer. *Bild: Truth Social, Gettr*

Telegram und das Recht

Im August tauchte bei vielen deutschen Telegram-Nutzern eine Umfrage auf, die das Verhältnis des Dienstes zu Recht und Gesetz gut veranschaulicht. Die Nutzer sollten darüber abstimmen, ob und unter welchen Voraussetzungen der Messenger Daten an Sicherheitsbehörden weitergeben soll. Die Umfrage bezog sich auf die seinerzeitige Datenschutzerklärung des Dienstes, nach der er IP-Adressen und Telefonnummern von Terrorverdächtigen an Behörden herausgebe, sofern ein gültiger Gerichtsbeschluss vorliegt. Zu den Antwortoptionen zählte, dass Telegram Nutzerdaten auch bei weniger schweren Straftaten ohne richterlichen Beschluss herausgeben soll – oder unter keinen Umständen, unabhängig von der Schwere der Straftat.

Dabei ist hierzulande per Netzwerkdurchsetzungsgesetz klar geregelt, unter welchen Umständen Anbieter wie Telegram Nutzerdaten herausgeben müssen – wie in vielen anderen Ländern auch. Telegram entzieht sich dem Zugriff durch Justiz und Regierungen allerdings durch seinen Sitz in Dubai. Das macht die Plattform zu einem wichtigen Kommunikationskanal für Oppositionelle in Ländern wie Iran, Belarus oder Syrien. In Deutschland ist Telegram allerdings auch ein Sammelbecken für Nazis, Corona-Leugner und Querdenker aller Art. In öffentlichen Telegram-Kanälen wird schon mal offen zu Gewalt aufgerufen, in kleineren Gruppen wurden Mordanschläge geplant.

Telegram wollte von seinen Nutzern in Deutschland wissen, unter welchen Umständen sie dem Dienst gestatten würden, Daten weiterzugeben. *Bild: Telegram*

Das Justizministerium hat schon vor 2022 massiv Druck auf Telegram ausgeübt, etwa indem es Bußgelder androhte und den Dienst mit Löschaufforderungen flutete. Seit Mitte des Jahres arbeitet Telegram offenbar mit dem BKA zusammen – ein wenig. So lösche der Dienst einen Großteil der Inhalte, um deren Löschung das Bundesinnenministerium ihn ersucht, so das Ministerium auf Anfrage von heise online. Und: „Durch das Bundeskriminalamt wurden Bestandsdatenanfragen in herausgehobenen Einzelfällen an Telegram übermittelt. Ein Teil dieser Anfragen wurde von Telegram beantwortet, zu einem kleinen Teil mit Bestandsdaten."

Diktaturen vs. Social Media

Wo immer Autokratien oder andere repressive Regierungen die Presse- und Meinungsfreiheit beschneiden, haben sie auch die sozialen Medien im Visier. Diese bieten in solchen Ländern oft die einzigen Plattformen, in denen sich Oppositionelle austauschen können. Das zeigte sich bei den Protesten gegen die althergebrachte Rolle der Frauen in Iran. Twitter, Facebook und Facebook Messenger, Telegram und Signal wurden in dem Land schon vor 2022 blockiert, ebenso wie der Zugriff auf

das anonymisierende Tor-Netzwerk.

Nachdem Mitte September landesweite Proteste aufflammten, hat das Regime auch WhatsApp und Instagram blockiert. Der mobile Internet-Zugang wurde vor allem in den Abendstunden komplett abgeschaltet. Die Regierung plante sogar, die Internetsperren dauerhaft beizubehalten. Dafür hätten sie einen enormen Flurschaden für die iranische Wirtschaft in Kauf genommen.

Die russischen Behörden haben im Zuge des Ukraine-Krieges nach und nach viele soziale Medien gesperrt, etwa Facebook, Instagram und Twitter. Andere soziale Medien waren das ganze Jahr über weiter in Russland aktiv, etwa YouTube und TikTok. Statt sie vollständig zu verbannen, überzogen die Behörden sie aber immer wieder mit Strafgeldern, etwa wenn sie missliebige Inhalte wie „Fehlinformationen“ über den Krieg in der Ukraine nicht gelöscht haben.

Zugleich hat es eine große und komplexe russische Desinformationskampagne im Westen gegeben. Die Operation begann im Mai, so der Rechercheverbund correctiv. Dabei wurden die Websites großer Medien täuschend echt nachgebaut, darunter der Spiegel, die Süddeutsche, der Tagesspiegel, Bild, T-Online und Welt. Auf diesen Sites wurden Fakes über die Ukraine verbreitet. Die gefälschten Inhalte wurden über Facebook, Instagram, Telegram und Twitter gestreut und sollten Stimmung gegen die Ukraine und ukrainische Flüchtlinge in Europa machen. Im September identifizierte und blockierte der Meta-Konzern Hunderte Facebook-Accounts und Facebook-Seiten und mehrere Dutzend Instagram-Accounts, die zu der Kampagne gehörten.

Gefährliche Inhalte

Trollarmeen oder andere Nutzer aufzuspüren und zu sperren, die politische Propaganda und Fake News verbreiten: Das gehört schon seit einigen Jahren zum Tagesgeschäft sozialer Medien. Bei besonderen Ereignissen verschärfen sie schon mal ihre

Nutzungsregeln, um Missbrauch zu unterbinden. Vor dem Hintergrund des Ukraine-Krieges hat Twitter sich zum Beispiel neue Richtlinien zu Desinformation in Krisenzeiten gegeben.

Der Fokus liege dabei laut dem sozialen Netzwerk auf Twitter-Konten mit hoher Reichweite wie Staatsmedien oder Konten staatlicher Institutionen. Bei ihnen sei die Wahrscheinlichkeit hoch, dass sie in Krisenzeiten angesteuert werden. Sollte es bei einem Tweet dort Hinweise darauf geben, dass er Falschinformationen enthält, dann empfiehlt Twitter ihn nicht und schaltet ihm einen Warnhinweis vor, dass er Falschinformationen enthält.

2022 sind soziale Medien, allen voran TikTok, allerdings auch wegen anderer Inhalte in den Fokus geraten: solche, die Kindern und Jugendlichen schaden. Die Justizminister mehrerer US-amerikanischer Bundesstaaten haben im März eine breite Untersuchung gestartet, die den Einfluss des Kurzvideo-Netzwerks auf Jugendliche und Heranwachsende analysiert.

Sie gehen davon aus, dass TikToks Algorithmen bei Jugendlichen und Kindern Essstörungen sowie sogar Selbstverletzungen und Selbstmord fördern können. Kritiker verweisen etwa auf Vorfälle in den USA, bei denen Schüler voriges Jahr Schultoiletten und andere Einrichtungen mutwillig zerstörten und Lernmaterialien stahlen – offenbar als Reaktion auf sogenannte Challenges auf der Plattform.

Tendenziöse Suche

Der Trend, TikTok als Suchmaschine zu nutzen, ist ebenfalls nicht harmlos. Denn die TikTok-Suche verbreitet auch Falschinformationen, etwa zum Thema Abtreibung oder zu den US-Wahlen. Das zeigt eine aktuelle Studie der Faktencheck-Initiative NewsGuard. Demnach enthalte fast jedes fünfte TikTok-Suchergebnis Falschinformationen. Für die Studie wurden im September 2022 für 27 Themenbereiche jeweils die Top 20 Suchergebnisse auf TikTok analysiert, etwa zu den

(englischsprachigen) Suchbegriffen „Wahl 2022“ oder „mRNA Impfstoff“.

Die Studie offenbarte ein weiteres Problem: Die Vorschläge in TikToks Suchmaske waren oft tendenziös. Bei den Suchbegriffen „Corona und Impfstoff“ schlug TikTok etwa vor, nach „Corona Impfstoff Wahrheit“ zu suchen. Bei „Klimawandel“ erschienen die Vorschläge „Klimawandel entlarvt“ und „Klimawandel gibt es nicht“. Gegenüber NewsGuard erklärte ein TikTok-Sprecher, dass schädliche Falschinformationen laut TikToks Community-Richtlinien nicht zugelassen seien und entfernt würden.

Ausblick: unmöglich

Im schnelllebigen Social-Media-Geschäft eine Prognose für das nächste Jahr abzugeben, ist so gut wie unmöglich. Allenfalls kann man einige Fragen für das nächste Jahr stellen: Werden TikTok und BeReal weiter so boomen wie bisher? Oder kommt ein neuer Wettbewerber, den man heute noch gar nicht auf dem Schirm hat, mit einer neuen Idee? Vielleicht wird 2023 auch das Jahr von Mastodon und dem Fediverse, die bislang eher eine Nische besetzt haben. Wenn Elon Musk allerdings Twitter weiter so konsequent herunterwirtschaftet, wären diese verteilten Netzwerke mögliche Ziele für Twitter-Emigranten. *(jo@ct.de)*

Elektronisches Bezahlen am Scheideweg

Europäisch oder amerikanisch?

Deutschland will der US-Konkurrenz beim Bezahlen in Läden und Onlineshops Paroli bieten. Doch bislang kommen Dienste wie Giropay oder ein paneuropäisches System trotz des Booms bei elektronischen Zahlungen nicht richtig in Fahrt. Gelingt ihnen keine Trendwende, drohen Verbrauchern auf Dauer höhere K…

Elektronisches Bezahlen am Scheideweg

Deutschland will der US-Konkurrenz beim Bezahlen in Läden und Onlineshops Paroli bieten. Doch bislang kommen Dienste wie Giropay oder ein paneuropäisches System trotz des Booms bei elektronischen Zahlungen nicht richtig in Fahrt. Gelingt ihnen keine Trendwende, drohen Verbrauchern auf Dauer höhere Kosten.

Von Markus Montz

kompakt

- Elektronische Zahlungen laufen dem Bargeld zunehmend den Rang ab.
- Amerikanische Finanzunternehmen haben in diesem Sektor eine starke Position, die marktbeherrschend werden und zu höheren Kosten führen könnte.
- Ob deutsche Dienste wie die Girocard und Giropay oder gesamteuropäische Systeme wie der digitale Euro mithalten werden, entscheidet sich wohl 2023.

Kunden greifen immer öfter zu elektronischen Bezahlmitteln. Das wollen verschiedene Akteure für sich ausnutzen, schließlich geht es um ein lukratives Geschäft. Bislang können sich nationale Bezahlmethoden in Deutschland und vielen europäischen Ländern gegen die Konkurrenz aus den USA behaupten. Doch der Wettbewerb wird immer intensiver und die amerikanischen Branchenriesen Mastercard, Visa und PayPal streben nach einem höheren Marktanteil.

Immerhin haben die Deutschen und die Europäer noch einige Asse auf der Hand. So will die Deutsche Kreditwirtschaft (DK) die Girocard – die frühere EC-Karte – digitalisieren und Giropay runderneuern, um besser mit den Amerikanern mithalten zu können. Was zunächst nach einem Problem von Kreditinstituten und Zahlungsdienstleistern klingt, hat handfeste Auswirkungen auf das Portemonnaie jedes Einzelnen. Unser Ausblick auf die nächsten Jahre zeigt daher nicht nur, wohin die Reise an den Kassen in Läden und Onlineshops gehen könnte, sondern auch warum Marktkonzentrationen problematisch sind und Bargeld weiterhin wichtig bleibt.

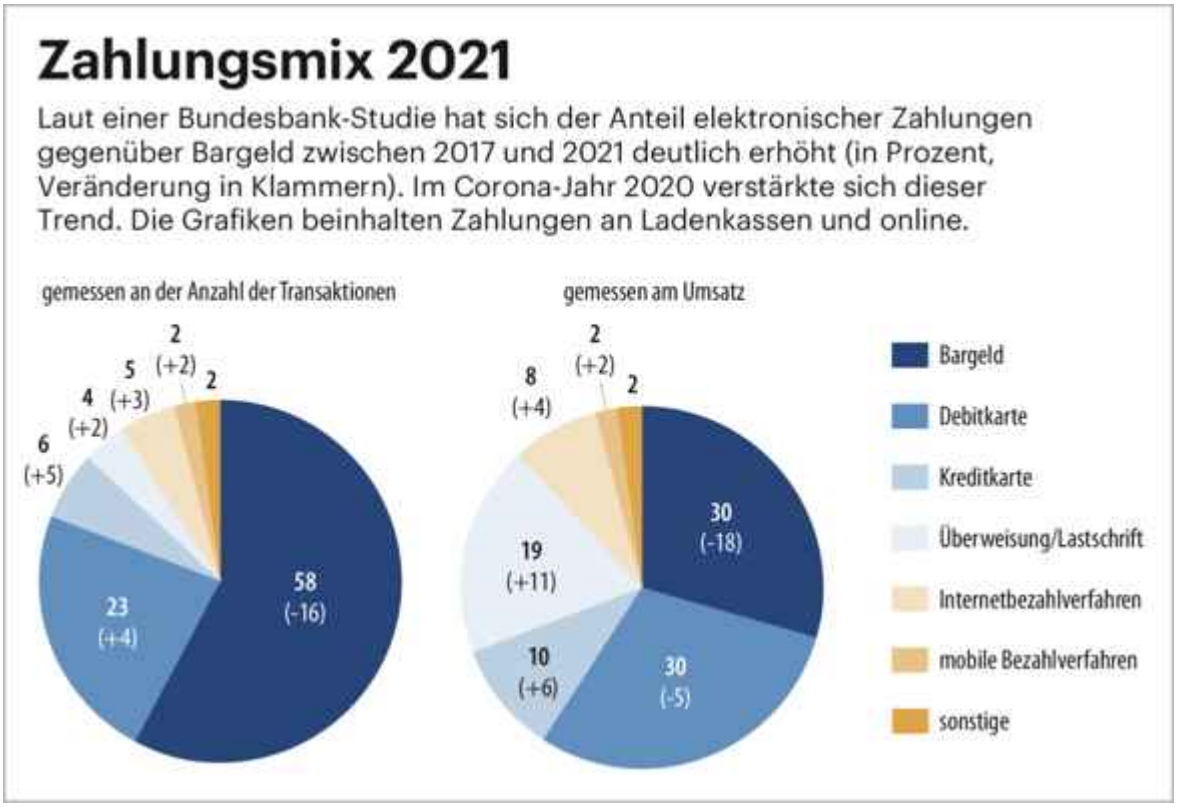
Karte statt Papier und Metall

Über allen Trends beim Bezahlen in Deutschland steht, dass Kunden ihre Einkäufe immer häufiger elektronisch zahlen – nicht nur in den boomenden Onlineshops, sondern auch an den Ladenkassen. Gemessen an den Bezahlvorgängen greifen die Menschen zwar noch bei über der Hälfte aller Einkäufe zu

Bargeld, der Vorsprung schmilzt aber deutlich ab. Gemessen am Umsatz hatten Bezahlkarten das Bargeld bereits 2020 überholt. Die aussagekräftigen Studien der Bundesbank bestätigen den allgemeinen Trend.

Die Corona-Pandemie spielt bei dieser Entwicklung eine wichtige Rolle und hat das bargeldlose Bezahlen an der Ladenkasse 2020 deutlich beschleunigt – vor allem durch den kontaktlosen Einsatz von Karten. Obwohl sich der Trend 2021 im Vergleich zu 2020 verlangsamt hat, ist eine Umkehr nicht zu erwarten. Das mag auch daran liegen, dass die Bargeldabwicklung für Händler zunehmend teurer wird und ihre Kosten für Kartenzahlungen in der Tendenz gesunken sind. Gerade Girocard-Zahlungen sind ab höheren zweistelligen Beträgen oft günstiger als Bargeld.

Dennoch wollen die meisten Bundesbürger nicht gänzlich auf Scheine und Münzen verzichten. Genau wie viele Verbraucherschützer nennen sie immer wieder diese Vorteile: Der Zahlvorgang ist anonym und schließt keine gesellschaftliche Gruppe aus. Nicht zuletzt macht Bargeld Ausgaben für viele Menschen nach wie vor überschaubarer als elektronische Verfahren. Es ist im Vergleich resilienter gegen Soft- und Hardwarefehler sowie Cyberangriffe und wirkt außerdem als wirtschaftliches und geopolitisches Machtkorrektiv gegen große Finanzkonzerne: Solange es Bargeld gibt, können diese nicht beliebig an der Gebührenschraube drehen. Zudem können Regierungen Bargeldflüsse schlechter kontrollieren oder sanktionieren als digitale Zahlungssysteme. All das wissen auch Politik und Finanzsektor. Dort spricht sich ebenfalls eine deutliche Mehrheit dagegen aus, Bargeld abzuschaffen.



Harte Zeiten für die Girocard

Bislang gewann unter den Debitkarten vor allem die deutsche Girocard im Zahlungsmix Marktanteile vom Bargeld – und das, obwohl man sie in der Regel nur an Kartenterminals nutzen kann. Gegenüber den Debitkarten der US-Konkurrenz von Mastercard und Visa hatte sie bisher den Vorteil, dass sie meist Teil des Girokonto-Paketes der Bank war. Da die Girocard ein System der Deutschen Kreditwirtschaft (DK) ist, bleiben Bezahldaten zudem bei der kartenausgebenden Bank und damit in Deutschland.

Händler wiederum schätzen an der Girocard die vergleichsweise niedrigen Entgelte, die sie bei Kartenzahlungen ihrer Kunden entrichten müssen. Da die Debitkarten von Visa und Mastercard wesentlich teurer sind, akzeptieren viele inhabergeführte Geschäfte sie bisher nicht – nach Schätzungen des Handelsverbands Deutschland betrifft das etwa 10 bis 20 Prozent aller 1,1 Millionen Kartenterminals im Einzelhandel. Was Inhabern dieser Karten Probleme bereiten kann, kommt Kunden insgesamt durchaus zugute: Schließlich legen Händler

die Kosten für die Zahlungssysteme auf die Produktpreise um.

Doch die US-Konkurrenz bläst zum Angriff [1]. Sie nutzt zwei Schwächen der Girocard: Man kann sie bislang weder online noch im Ausland einsetzen. Für den zweiten Fall statten die meisten Banken die Girocard mit einem zweiten Debitkartensystem aus (Co-Badge) – dem auf Europa beschränkten „V Pay“ von Visa oder alternativ dem weltweit gültigen „Maestro“ von Mastercard. Mastercard lässt „Maestro“ jedoch ab Juli 2023 auslaufen.

Ohne Co-Badge benötigen Girocard-Inhaber im Ausland eine zweite Karte. In der Regel ist dies eine Debit- oder Kreditkarte für die Hauptsysteme von Mastercard und Visa. Solch eine zweite Karte kostet Banken jedoch zusätzlich Geld in der Produktion, das sie sich in der Regel von ihren Kunden zurückholen. Vor allem Direktbanken sparen sich die Zusatzkosten und geben für ihre Girokonten standardmäßig Debitkarten von Visa und Mastercard aus, mit denen man außerdem im Internet einkaufen kann. Wünscht der Kunde trotzdem eine Girocard, muss er diese oft extra bezahlen. Viele Sparkassen und Volks- und Raiffeisenbanken probieren einen Spagat und kombinieren die Girocard mit einer Debitkarte von Visa- oder Mastercard. Ob und wie sich das auf die Kontoführungsgebühren auswirkt, muss sich noch zeigen.

Ab 2023 könnte die Girocard erstmals Marktanteile verlieren: Je mehr Kunden künftig statt der Girocard eine Debitkarte von Visa und Mastercard nutzen, desto mehr Einzelhändler könnten sich auch gezwungen sehen, diese zu akzeptieren. Das könnte viele kartenherausgebende Banken (Issuer) neu kalkulieren lassen. Schließlich verdient abgesehen von der Händlerbank (Acquirer) und den Kartenfirmen bei jeder Zahlung mit einer Debitkarte von Visa und Mastercard auch der Issuer Geld: Er erhält 0,2 Prozent vom Umsatz. Bei der Girocard bekommt die kartenausgebende Bank hingegen einige Promille weniger.

Visa und Mastercard schütten ihre Gewinne nicht nur an die Aktionäre aus, sondern nutzen sie auch, um neue Bezahlmethoden

und Standards zu entwickeln. Ralf Gladis vom Zahlungsabwickler Computop (siehe Interview auf S. 153) nennt als Beispiele Verfahren, bei denen Nutzer sich biometrisch authentifizieren oder Dienstleister Kartendaten als geräte- oder händlergebundene Zufallswerte (Token) speichern. Dadurch können Verbraucher bequem elektronisch zahlen, ohne Abstriche beim Schutz gegen Kartenmissbrauch machen zu müssen. Um mit Visa und Mastercard konkurrieren zu können, muss die Deutsche Kreditwirtschaft (DK) die Girocard rasch weiter ausbauen.

Der Einsatz der deutschen Girocard im Ausland ist in der Regel an die Debitkartendienste Maestro (von Mastercard, weltweit) und V Pay (von Visa, in Europa) gebunden. Mastercard und Visa wollen nun jedoch ihre eigenen Debitkarten stärker im deutschen Markt etablieren.


V
PAY
Debit
maestro


VISA
Debit

Girocard, Giropay – alles neu?

Dazu will die DK nun die Girocard fit für Onlinezahlungen machen und gleichzeitig ihre Bezahlverfahren Giropay, Paydirekt sowie die Person-to-Person-(P2P-)Zahlungsfunktion Kwitt unter der Marke Giropay zusammenfassen. Wenn das klappt, könnten sie nicht nur Visa und Mastercard, sondern künftig auch PayPal Paroli bieten.

Ab 2023 wollen zunächst die Sparkassen sowie die Volks- und Raiffeisenbanken ihre Android-Bezahl-Apps in Wallets umwandeln. Damit wären Girocard-Inhaber nicht mehr auf Ladenkassen beschränkt, sondern könnten auch Zahlungen in Onlineshops abwickeln. Unklar ist bislang, ob weitere Banken digitale Girocards einführen und ob diese am Ende auch mit iPhones funktionieren. Bislang sind Girocard-Zahlungen unter iOS nur für Sparkassen-Kunden über den Umweg mit Apple Pay

möglich.

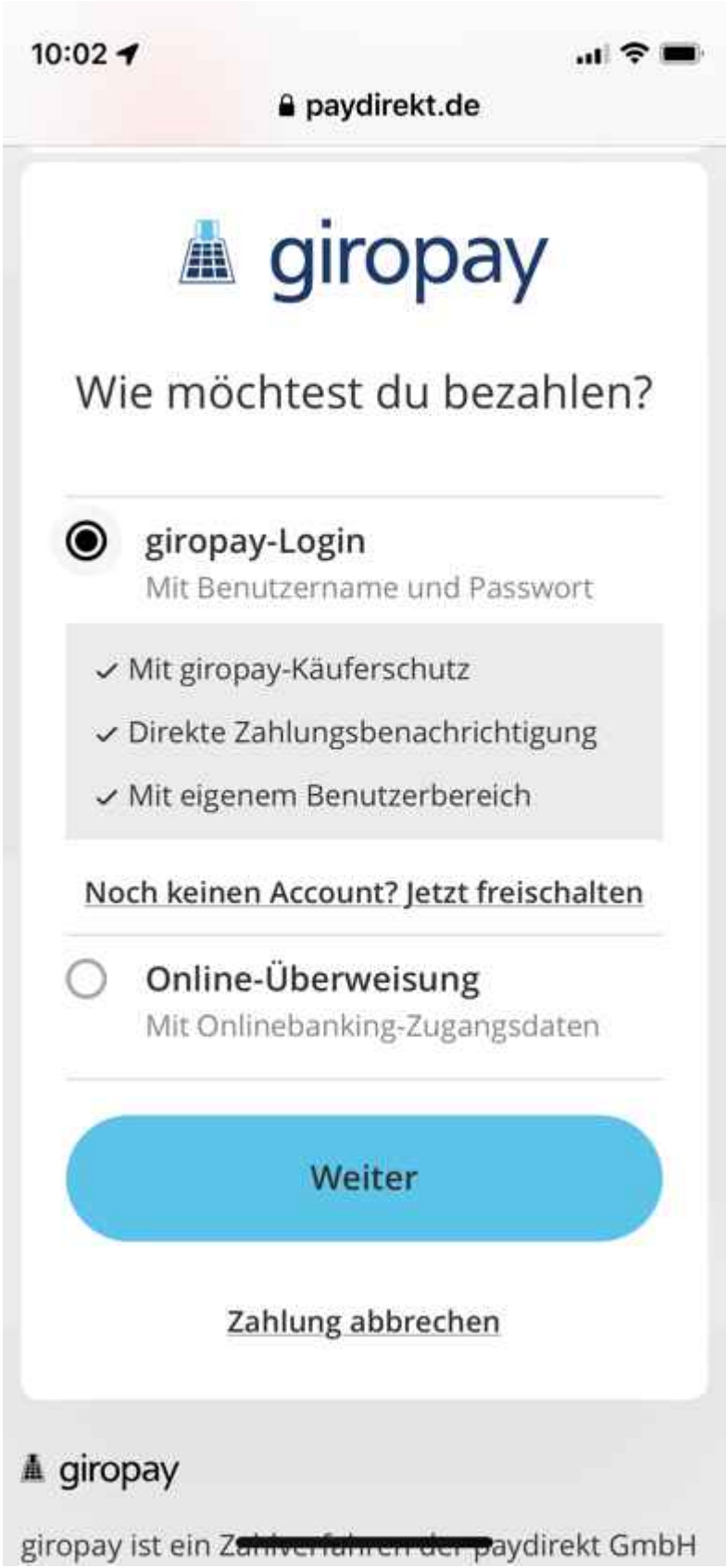
Das neue Giropay ist anders als die Girocard für Zahlungen in Webshops gedacht. Bei diesen Zahlungen wählt man während des Zahlungsvorgangs aus, ob man das Überweisungsschema des alten Giropays nutzt oder mit dem bisher unter „Paydirekt“ firmierenden Verfahren mittels Mailadresse und Passwort zahlen möchte [2]. Unklar ist noch, wie die DK das P2P-Bezahlverfahren Kwitt in Giropay integrieren wird. Bislang binden teilnehmende Banken es als Funktion in ihre Banking-Apps für das Smartphone ein; Nutzer können dann Geld an Kontakte in ihrem Adressbuch über deren Handynummern schicken.

Der Erfolg von Giropay und der digitalen Girocard hängt davon ab, ob sie den Verbrauchern erkennbare Vorteile gegenüber etablierten Zahlverfahren bieten. Damit sind nicht nur PayPal, Mastercard und Visa gemeint, sondern auch Rechnungskauf und Lastschrift. Kwitt hat allein PayPal als Gegner. Der Konzern wickelt derzeit aber über 90 Prozent aller P2P-Zahlungen in Deutschland ab; außerdem kann man mit PayPal anders als mit Kwitt auch private und gewerbliche Käufe komfortabel nach dem P2P-Prinzip bezahlen und ist nicht an das Smartphone und dessen Adressbuch gebunden.

Mastercard und Visa wollen den Bezahlprozess im Internet ebenfalls vereinfachen. Auch sie bringen derzeit Wallets auf den Markt („Click to pay“). Kunden müssen damit nicht mehr umständlich die 16-stellige Kartennummer eintippen, sondern geben beim Händler lediglich eine Mailadresse an. Anschließend authentifizieren sie sich mit Passwort, Gesichtsscan oder Fingerabdruck auf ihrem Smartphone.

Dass nationale Bezahlverfahren in Europa es durchaus mit der US-amerikanischen Konkurrenz aufnehmen können, zeigen P2P-Bezahlsysteme wie Twint in der Schweiz oder Mobile Pay in Dänemark. Genau wie Kwitt binden sie das Girokonto ihrer Kunden direkt ein, statt einer Kontonummer genügt die Handynummer des Empfängers – dieser muss allerdings nicht im

Adressbuch des Smartphones stehen. Twint und Mobile Pay eignen sich daher anders als Kwitt auch für private und gewerbliche Verkäufer im Einzelhandel sowie im Internet, Käuferschutz inklusive. Beide Systeme sind zudem preisgünstiger als Mastercard, Visa oder PayPal. Um gegen die US-Konkurrenz eine Chance zu haben, müsste die DK den Bezahlvorgang für Girocard und Giropay ähnlich einfach gestalten wie Twint und Mobile Pay und weiterhin günstiger für Händler bleiben als die US-Konkurrenz.



Mit einem runderneuerten Giropay will die Deutsche Kreditwirtschaft PayPal und den Kartenkonzernen Visa und Mastercard Konkurrenz machen. Dem steht bislang allerdings der begrenzte P2P-Funktionsumfang im Weg.

Streit um europäische Bezahlsysteme

Auch auf europäischer Ebene planen Banken und Sparkassen ein Bezahlsystem. Im Unterschied zu Giropay und Girocard soll man damit auf Basis der SEPA-Echtzeitüberweisung überall in Europa bezahlen können. Dafür hatten 2020 zunächst 16 europäische Banken die „European Payments Initiative“ (EPI) gegründet. Wenig später traten ihr 14 weitere Institute sowie zwei Zahlungsabwickler bei.

Nach Differenzen über die Strategie und Finanzierung wollen noch elf Institutionen aus Deutschland, Frankreich, Belgien und Spanien sowie die Zahlungsabwickler aus Italien und Frankreich das Projekt weiterführen. Aus Deutschland sind die Sparkassen-Gruppe und Deutsche Bank vertreten. Nutzer sollen anders als ursprünglich geplant keine Plastikkarte, sondern einzig ein Wallet bekommen. Wie bei PayPal soll man damit online bezahlen und zusätzlich über eine Smartphone-App auch Geld abheben können [3]. Die Entscheidung über den Start sollte ursprünglich im Mai 2022 fallen, zuletzt war von November die Rede.

Vielleicht finden aber die 15 nationalen Bezahldienste eine Lösung, die im Rahmen der European Mobile Payment Systems Association (EMPSA) auf europäische Interoperabilität setzen: Der Nutzer eines Dienstes aus Spanien zum Beispiel soll auch bei Händlern in Schweden bezahlen können und umgekehrt. An Bord ist unter anderem das aus Österreich stammende Bluecode, das bereits jetzt Händlern und Verbrauchern in Deutschland offensteht. Noch 2022 sollen alle Bluecode-Nutzer mit ihrem Smartphone auch an Kassen in der Schweiz bezahlen können, die Twint akzeptieren. Bis zu einer Interoperabilität zwischen allen 15 beteiligten Diensten wird es allerdings dauern, weil diese zunächst Technik, Zahlungsabwicklung sowie Daten- und Betrugsschutz organisieren müssen.

Unklare Chancen für Open Banking

Eher langsam geht es bisher auch beim Open Banking voran, das den US-Riesen ebenfalls Konkurrenz machen soll. Dienste wie Giropay und Klarnas „Sofortüberweisung“ fristen bei Bezahlvorgängen im Internet bisher ein Nischendasein. Viele Kunden scheuen sich, einem Drittdienst auch nur begrenzten Zugriff auf ihr Konto zu gewähren [4]. Möglicherweise werden die Karten neu gemischt, wenn Überweisungen nicht erst nach einem Tag beim Empfänger sind, sondern die SEPA-Echtzeitüberweisung zum Normalfall wird. Bisher scheitert dies vor allem daran, dass zahlreiche Banken diese nicht anbieten. Wenn doch, müssen Bankkunden meist einen Aufschlag zahlen. Die EU-Kommission will die Banken jedoch dazu verpflichten, Echtzeitüberweisungen anzubieten, und die Aufschläge verbieten.

Das könnte auch SEPA Request to Pay helfen. Das Konzept hinter diesem Rahmenwerk des Europäischen Zahlungsverkehrsausschusses ähnelt dem Open Banking: Der Zahlungsdienstleister des Händlers schickt der Bank des Kunden eine Zahlungsaufforderung, die diese dem Kunden ins Onlinebanking stellt. Bestätigt er diese Aufforderung, geht das Geld von seinem Konto an den Händler. Das Verfahren eignet sich für den Internethandel, es wäre in Kombination mit der SEPA-Echtzeitüberweisung und der Banking-App auf dem Smartphone aber auch an Ladenkassen denkbar.

Neue Regeln für Ratenzahlungen

Auch für „Buy now, pay later“, die hip verpackten Rechnungs- und Ratenkäufe, sind 2023 Veränderungen zu erwarten. Das Geschäftsmodell, das vor allem Zahlungsdienstleister wie Klarna oder PayPal vorantreiben, steht seit Jahren in der Kritik [6]. Verbraucherschützer werfen vor allem Klarna vor, durch sein aggressives Marketing gezielt Menschen mit unterdurchschnittlicher Wirtschaftskraft und Finanzbildung anzusprechen, speziell junge Erwachsene. Derzeit verhandeln

EU-Kommission, -Parlament und -Rat über eine neue, verschärfte Verbraucherkreditrichtlinie, die Klarna & Co. das Geschäft künftig erschweren könnte. Im Gespräch sind strengere Kreditwürdigkeitsprüfungen, transparentere Information über Kreditkosten sowie ein Zinsdeckel.

Unabhängig davon bleibt die Frage, ob Verbraucher in der Wirtschaftskrise tendenziell stärker auf Ratenkäufe für Konsumgüter setzen und sich womöglich öfter finanziell übernehmen oder ob sie Verzicht üben. Clas Beese vom Branchendienst Finletter weist auf einen möglichen Gegentrend hin: Bei „Save now, buy later“ – „Spare jetzt, kaufe später“ – versuchen Finanz-Start-ups und Banken, ihre Klientel gezielt und mit spielerischen Elementen zum Sparen auf ihre Wünsche zu bewegen, anstatt auf Pump zu kaufen.

Rettet es der digitale Euro?

Da sich Deutschland mit innovativen Zahlverfahren schwertut und ein paneuropäisches System auf die Schnelle kaum kommen wird, hoffen viele Experten auf den digitalen Euro [5]. Die Europäische Zentralbank (EZB) hat bereits erste Weichen gestellt und Mitte 2021 nach ersten technischen Experimenten die Machbarkeit verkündet.

Seither entwickelt die EZB in einer auf zwei Jahre angelegten „Untersuchungsphase“ gemeinsam mit Vertretern von Verbrauchern, Handel und Finanzwirtschaft verschiedene Konzepte. Diese prüfen sie auf gesellschaftlich relevante Auswirkungen, zum Beispiel für die Finanzstabilität oder die finanzielle Inklusion, sowie auf technische Aspekte wie Anonymität, Geldwäscheprävention und Sicherheit.

Erste Ergebnisse sollen im Laufe des Jahres 2023 vorliegen. Anschließend will die EZB einen Prototyp entwickeln, der 2025 in den Regelbetrieb gehen könnte. Der Zeitplan ist ambitioniert. Schließlich geht es nicht um ein Zahlverfahren, sondern um die Währung an sich. Hinzu kommt die Frage nach den

Vorteilen gegenüber bestehenden Zahlungsverfahren. An einer konstruktiven Auseinandersetzung mit digitalem Zentralbankgeld führt allerdings kein Weg mehr vorbei, seit China den digitalen Renminbi eingeführt hat. Sollte dieser auf globaler Ebene Wirkung entfalten, benötigt Europa ein Konzept, um seine finanzpolitische Eigenständigkeit sicherzustellen.

Auch zu Projekten privater Unternehmen braucht die EU ein Gegengewicht. Damit sind weniger die klassischen, dezentral organisierten Kryptowährungen wie Bitcoin gemeint. Sie taugen bereits wegen ihrer Kursschwankungen und ihres technischen Anspruchs absehbar nicht als Zahlungsmittel im Alltag. Vielmehr soll der digitale Euro es sogenannten „Stablecoins“ schwer machen. Zwar hat die europäische Politik Projekte wie den vom Meta-Konzern geplanten „Diem“ (ursprünglich „Libra“) durch hohe gesetzliche Auflagen vorerst verhindert. Dennoch könnten Unternehmen in den kommenden Jahren Konzepte entwickeln, die diese Auflagen erfüllen – mit unbekannten Risiken für Finanzmärkte, Volkswirtschaften und damit auch für Verbraucher.

Ausblick

Zurzeit spricht mehr dafür, dass die US-Finanzkonzerne ihre Position in Deutschland in den kommenden Jahren zulasten der nationalen Systeme ausbauen und den Trend zu mehr elektronischen Zahlungen für sich nutzen können. Die neuen, aus Verbrauchersicht sehr begrüßenswerten Strategien für Girocard und Giropay kommen spät und scheinen nicht breit genug aufgestellt. Nach aktuellem Stand bieten sie auch in runderneuerter Form zu wenige Vorteile gegenüber Mastercard, Visa und PayPal.

Dass deren höhere Entgelte für Händler die Preise beeinflussen, ist für Verbraucher zu wenig ersichtlich. Diese Intransparenz macht eine europäische Alternative wie EPI umso nötiger – nicht zuletzt, um den Wettbewerb unter den Bezahlsystemen anzukurbeln und die Bildung von Kartellen oder

Oligopolen zu verhindern. Dass dieses Ziel keineswegs verwegen ist, zeigen viele europäische Länder mit ihren komfortablen, sicheren und preisgünstigen nationalen P2P-Bezahlsystemen. Ein ähnliches Gegengewicht zu den US-Riesen wäre auch für Deutschland ein Gewinn und käme Handel, Banken und insbesondere den Verbrauchern zugute. *(mon@ct.de)*

Glossar

Acquirer/Händlerbank: Stellt dem Händler den Anschluss an die Systeme z.B. von Girocard, Mastercard oder Visa her und wickelt Zahlungen für ihn ab.

Co-Badge: Ein sekundäres Bezahlsystem auf einer Bezahlkarte, das zum Einsatz kommt, wenn das Kartenlesegerät das primäre System nicht unterstützt – erkennbar am zweiten (Co-)Symbol (Badge).

Debitkarte: Bezahlkarte, bei der die Bank das Geld innerhalb weniger Tage vom Konto abbucht (also ohne Aufschub wie bei Kreditkarten).

Deutsche Kreditwirtschaft (DK): Spitzenverband der deutschen Banken und Sparkassen, unter anderem für Standards und Spezifikationen im Zahlungsverkehr zuständig.

Digitaler Euro: Möglicherweise in der Zukunft von der Europäischen Zentralbank ausgegebenes, ausschließlich für digitale Zahlungen vorgesehenes Währungsäquivalent zum Euro.

Echtzeitüberweisung: Vom Europäischen Zahlungsverkehrsausschuss spezifiziertes Überweisungsverfahren, bei dem die Banken dem Empfänger im einheitlichen europäischen Zahlungsraum (SEPA) eine Überweisung nach spätestens zehn Sekunden gutschreiben müssen.

European Mobile Payment Systems Association (EMPSA): Europäischer Mobilzahlungssysteme-Verband; die darin organisierten 15 nationalen Mobilzahlungsdienste wollen ihre

Systeme europaweit interoperabel machen.

European Payments Initiative (EPI): Projektname für ein geplantes paneuropäisches Bezahlverfahren mittels Wallet. Ein Bankenkonsortium will es im gesamten Euroraum zur Verfügung stellen.

Giropay: Internet-Bezahlverfahren der Deutschen Kreditwirtschaft, bei dem der Nutzer Geld an den Händler überweist und seine Bank den Händler darüber in Echtzeit informiert. Wird mit Paydirekt und Kwitt als „neues" Giropay zusammengeführt.

Issuer/Kartenherausgeber: Finanzinstitut, das eine Bezahlkarte (z.B. in den Systemen von Girocard, Mastercard, Visa) an den Kunden herausgibt.

Kryptowährung: Rein digitaler Geld- oder Vermögenswert bzw. digitales Zahlungsmittel, dessen einzelne Einheiten (Coins) und deren jeweilige Inhaber i.d.R. in einer dezentral organisierten Datenbank geführt werden.

Kwitt: P2P-Zahlungsverfahren in Banking-Apps auf dem Smartphone. Nutzer können anderen Nutzern, deren Handynummer sich im Adressbuch befindet, direkt Geld schicken.

Mobile Pay: Dänisches, auf eine Smartphone-App gestütztes System für P2P- und elektronische Zahlungen; Nutzer senden Geld über die Handynummer des Empfängers oder zahlen über eine im Webshop oder der Kasse integrierte Funktion.

Maestro: Weltweites Debitkartensystem von Mastercard; primär für den stationären Handel und Geldautomaten konzipiert. Läuft ab Juli 2023 bis Juni 2027 zugunsten der „Mastercard Debit" aus.

Open Banking: Vom Kunden genehmigter Zugriff von Drittdiensten auf dessen Girokonto. Anbieter – sogenannte Kontoinformations- und Zahlungsauslösedienste – benötigen eine Erlaubnis der

Finanzdienstleistungsaufsicht. Beispiele: „Sofortüberweisung“, seit 2014 Teil von Klarna, und das klassische Giropay.

Paydirekt: Internet-Bezahlverfahren der Deutschen Kreditwirtschaft, mit dem Kunden mittels Nutzername und Passwort in Onlineshops bezahlen können; firmiert mittlerweile unter „Giropay“.

P2P-Zahlung: Elektronische „Person-to-Person“-(P2P-)Geldtransaktion zwischen zwei Wallets, bei der an die Stelle der Kontonummer des Empfängers i.d.R. dessen Mailadresse oder Handynummer tritt.

Stablecoin: Kryptowährungen, die an Zentralbankwährungen wie den Dollar oder Euro gekoppelt und durch Rücklagen oder Vermögenswerte gedeckt sind.

Twint: Schweizerisches, auf eine Smartphone-App gestütztes System für P2P- und elektronische Zahlungen; Nutzer senden Geld über die Handynummer des Empfängers oder zahlen über eine im Webshop oder der Kasse integrierte Funktion.

V Pay: Debitkartensystem von Visa für Europa, für den stationären Handel und Geldautomaten konzipiert; konkurriert intern mit der „Visa Debit“.

Wallet: Digitale Brieftasche für elektronische Zahlungen, in der man Bezahlkarten oder andere Zahlverfahren hinterlegt – Beispiele sind PayPal, Apple Pay und Google Pay.

„Ich teile den Wunsch nach einem europäischen Zahlungssystem“

Ralf Gladis ist Mitgründer und Geschäftsführer von Computop Paygate. Das Unternehmen bindet Händler technisch an Bezahlsysteme an und wickelt elektronische Zahlungen ab. Im Gespräch mit c’t gibt Gladis einen Ausblick auf die Trends der nächsten Jahre.

Der Trend zur Bargeldloszahlung hält an. Wird das Bargeld

verschwinden?

Ralf Gladis: Bargeld bleibt uns noch lange erhalten. In der Pandemie haben aber viele Konsumenten entdeckt, wie komfortabel kontaktloses elektronisches Bezahlen sein kann. Die Menge der elektronischen Zahlungen wächst seit Jahren mit zweistelligen Prozentwerten. Niemand wird das Bargeld von oben herab abschaffen, aber in Schweden etwa sehen wir, dass Handel und Konsumenten lieber darauf verzichten, selbst am Gemüsestand. Bargeld ist eben auch unbequem in der Beschaffung und teuer im Handling.

Könnten die Debitkarten von Mastercard und Visa die Girocard bald abhängen?

Gladis: Ob sich Visa und Mastercard mit ihren Debitkarten gegen die Girocard durchsetzen können, hängt davon ab, wie schnell die Banken die Girocard digitalisieren. Das ist bei Apple Pay mit Girocard schon erkennbar. Ohne europäisches System bleiben die Banken vorerst weiter auf die Zusammenarbeit mit Visa und Mastercard angewiesen, damit deutsche Karteninhaber ihre Girocard auch im Ausland einsetzen können.

Könnte das neue Giropay PayPal noch Konkurrenz machen?

Gladis: Wenn Giropay auch die Girocard in sein Bezahlsystem integriert, wird dessen Popularität erheblich steigen. Damit könnte Giropay Umsätze von PayPal gewinnen. Trotzdem: Für Händler bleibt PayPal attraktiv, weil dort Millionen Konsumenten weltweit registriert sind. Um deutsche Kunden, die sich an PayPal gewöhnt haben, von Giropay zu überzeugen, braucht es Zeit und günstige Preise. Außerdem ist stetige Innovation wichtig – so wie bei Visa und Mastercard mit ihren nun geplanten Wallets. Es rächt sich bis heute, dass die Banken Giropay zu spät und damals zu schwach in den Markt gebracht hatten.

Und wie sehen Sie die Chancen der European Payments Initiative

(EPI)?

Gladis: Ich teile den Wunsch nach einem europäischen Zahlungssystem, aber es fehlt in der Bankenwelt die Innovationskraft und die Fähigkeit, sich auf neue Standards zu einigen. Daher sehe ich für den Erfolg von EPI kaum eine Chance. Die Lücke könnte aber der digitale Euro füllen.

Haben Open-Banking-Varianten vielleicht mehr Potenzial?

Gladis: Mit Echtzeitüberweisungen vielleicht. Momentan bleiben aber zu viele Fragen unbeantwortet: Wie funktionieren Echtzeitüberweisungen an der Kasse? Wie authentifiziert sich der Kunde dafür unkompliziert im Onlineshop? Wer kümmert sich um Rückzahlungen oder Streit zwischen Händler und Kunde? Diese organisatorischen Themen haben Visa, Mastercard und PayPal bereits mit Regeln für alle Parteien gelöst.

Ist das auch eine Preisfrage?

Gladis: Die Kosten für Echtzeitüberweisungen sind für Kunden und für Händler oft unattraktiv, weil viele Banken abschreckende Preise dafür festgelegt haben. Man darf zudem nicht vergessen, dass die Banken mit Visa und Mastercard bereits profitable Geschäftsmodelle aufgebaut haben. Welche Motivation hätten sie, diese zu ersetzen? Und welche Motivation hat der Kunde, Echtzeitüberweisungen einzusetzen?

Kann der digitale Euro die Antwort sein?

Gladis: Mit dem digitalen Euro könnten wir erreichen, was EPI bisher nicht erreicht hat: Er könnte ein rein europäisches Zahlungsmittel werden. Ein digitaler Euro mit der EZB im Rücken hätte genug Vertrauen, um erfolgreich zu sein. Der Erfolg des digitalen Euro setzt aber voraus, dass man damit ähnlich einfach wie mit Bargeld zahlen kann. Ich hoffe sehr, dass die Pilotprojekte auf EU-Ebene zu guten Ergebnissen führen.

Können Digitalkonzerne mit ihrer Erfahrung beim Bedienkomfort das nicht ebenso gut, Stichwort „Diem“?

Gladis: Zu Diem habe ich als Bürger eine klare Meinung: Kein Privatunternehmen sollte die Kontrolle über eine starke Parallelwährung erhalten, denn das schränkt den wirtschaftspolitischen Handlungsspielraum unserer gewählten Politiker und der EZB ein. Das wäre eine Gefahr für unsere Demokratie.

Wie schätzen Sie das (Reiz-)Thema Ratenzahlungen („Buy Now, Pay Later“) ein? Wächst der Sektor weiter?

Gladis: Inflation und hohe Energiepreise senken auch die Nachfrage im Onlinehandel. Eine Ratenzahlung verschafft den Konsumenten zwar zusätzliche Liquidität, sodass wir bei Computop steigende Nachfrage nach Ratenzahlung sehen. Das birgt aber auch die Gefahr der Überschuldung. Insbesondere die Generation Z im Alter von 14 bis 21 Jahren ist wirtschaftlich eher fragil und sollte vor aggressiven Angeboten geschützt werden. Deshalb halte ich eine Regulierung für sinnvoll. Trotzdem würde ich meinen (Händler-)Kunden dringend raten, eine Ratenzahlung im Check-out anzubieten.

Ralf Gladis, Mitgründer und Geschäftsführer Computop Paygate
Bild: Bjoern Seitz

1. Literatur
2. Markus Montz, Kleines Logo, große Wirkung, Mit welcher Debitkarte Sie besser bezahlen: Girocard oder Visa und Mastercard, c’t 22/2022, S. 114
3. Markus Montz, Geld hin, Geld her, PayPal, Paydirekt, Kwitt: Bezahl-Apps im Vergleich, c’t 18/2022, S. 120
4. Markus Montz, Zahlungsverzug, European Payments Initiative am Scheideweg, c’t 7/2022, S. 46
5. Markus Montz, Geöffnete Geldhäuser, Wie Open Banking den Finanzsektor verändert, c’t 24/2021, S. 132
6. Tobias Weidemann, Ganz neues Geld, Der lange Weg zum digitalen Euro, c’t 4/2022, S. 108
7. Markus Montz, Jetzt kaufen, später zahlen? Wann man von Klarna, PayPal & Co. besser die Finger lässt, c’t 14/2022, S. 132

VPN-Überblick: Standorte vernetzen, Geoblocking und Zensur umgehen, Privatsphäre schützen

Verschlüsselte Wendungen

Virtual Private Networks gibt es heute für deutlich mehr Zwecke, als der Name vermuten lässt. In diesem Streifzug lesen Sie, wie diese vielfältige Softwaregattung entstand und dass sie neben soliden Ökosystemen auch sumpfige hervorbrachte. Außerdem geht es um Praxis zu einem mächtigen Mauerblümchen.
Virtual Private Networks gibt es heute für deutlich mehr Zwecke, als der Name vermuten lässt. In diesem Streifzug lesen Sie, wie diese vielfältige Softwaregattung entstand und dass sie neben soliden Ökosystemen auch sumpfige hervorbrachte. Außerdem geht es um Praxis zu einem mächtigen Mauerblümchen.

Von Dušan Živadinović

kompakt

- Viele VPN-Anwendungen haben den spröden Charm der Kommandozeile abgelegt und lassen sich komfortabel bedienen.
- Manche neuen VPN-Funktionen spiegeln gut wider, dass Anwendern der freie Internet-Zugang wichtig ist.
- Für den Privatsphärenschutz setzen Entwickler Techniken

ein, die sich bei digitalen Wahlmaschinen bewährt haben.

Ursprünglich hat man Virtual Private Networks (VPN) entwickelt, um entfernte Standorte miteinander zu vernetzen (Site-to-Site), später auch, um ferne Benutzer an Firmen- oder Heimnetze anzukoppeln (Road-Warrior, auch End-to-Site-VPNs genannt), und für diverse andere Zwecke. Zu den wichtigsten davon gehören VPN-Varianten für das Anonymisieren und das Umgehen von Geoblocking und Internet-Sperren (Tor) sowie den Privatsphärenschutz.

Mit Virtual Private Networks waren anfangs nur Routing- und Bridging-Programme zur Standortvernetzung gemeint. Zu Beginn der Internet-Ära koppelte man entfernte Netze sogar noch ohne jeglichen Kryptoschutz. Das änderte sich, nachdem klar wurde, dass über solche Verbindungen auch Daten fließen, die besser vertraulich bleiben.

Fortan blieb die Wahrung der Vertraulichkeit eine der wichtigsten Antriebsfedern und brachte immer neue kryptografische Absicherungen der Nutzdaten gegen unerwünschte Mitleser hervor. Unzureichend gehärtete VPN-Varianten, die ihre vertrauliche Fracht nicht vor Angreifern schützen konnten, verschwanden wieder von der Bildfläche. Ein Beispiel ist das von Microsoft entwickelte Point-to-Point Tunneling Protocol (PPTP), das zwar sehr einfach zu konfigurieren war, sich aber mit überschaubarem Aufwand knacken ließ (siehe ct.de/y9y1). PPTP hat in modernen Installationen nichts zu suchen.

Neben PPTP kamen diverse Spielarten von SSL-VPNs auf und erlangten große Verbreitung. Sie verschlüsseln Nutzdaten mittels Transport Layer Security (früher Secure Socket Layer, SSL, genannt). Bis heute sehr verbreitet sind Implementierungen, die ohne Clientsoftware funktionieren, weil sie sich besonders für den spontanen Aufbau gesicherter Verbindungen eignen (Tunnel), also etwa zwischen Webbrowsern

und Webservern. Viele tunneln aber nur den Verkehr bestimmter Anwendungen (z. B. Mailclient und -server, verschlüsselnde DNS-Clients und -Resolver), bieten also keine Infrastrukturvernetzung etwa für Dateifreigaben, weshalb ihre Einordnung zu VPNs umstritten ist.

Die bekannteste SSL-VPN-Spielart inklusive Netzwerkzugriff, also mit Kapseln kompletter IP-Pakete, ist bis heute das quelloffene OpenVPN. Jahrelang galt es als das am weitesten verbreitete VPN überhaupt. Daneben gibt es diverse weniger bedeutende SSL-VPNs etwa von Router-Herstellern wie Netgear. Neben OpenVPN galten lange Zeit nur das komplizierte, aber bis heute sichere IPsec und Varianten wie IPsec/L2TP als zuverlässige Alternative zur Netzwerkkopplung.

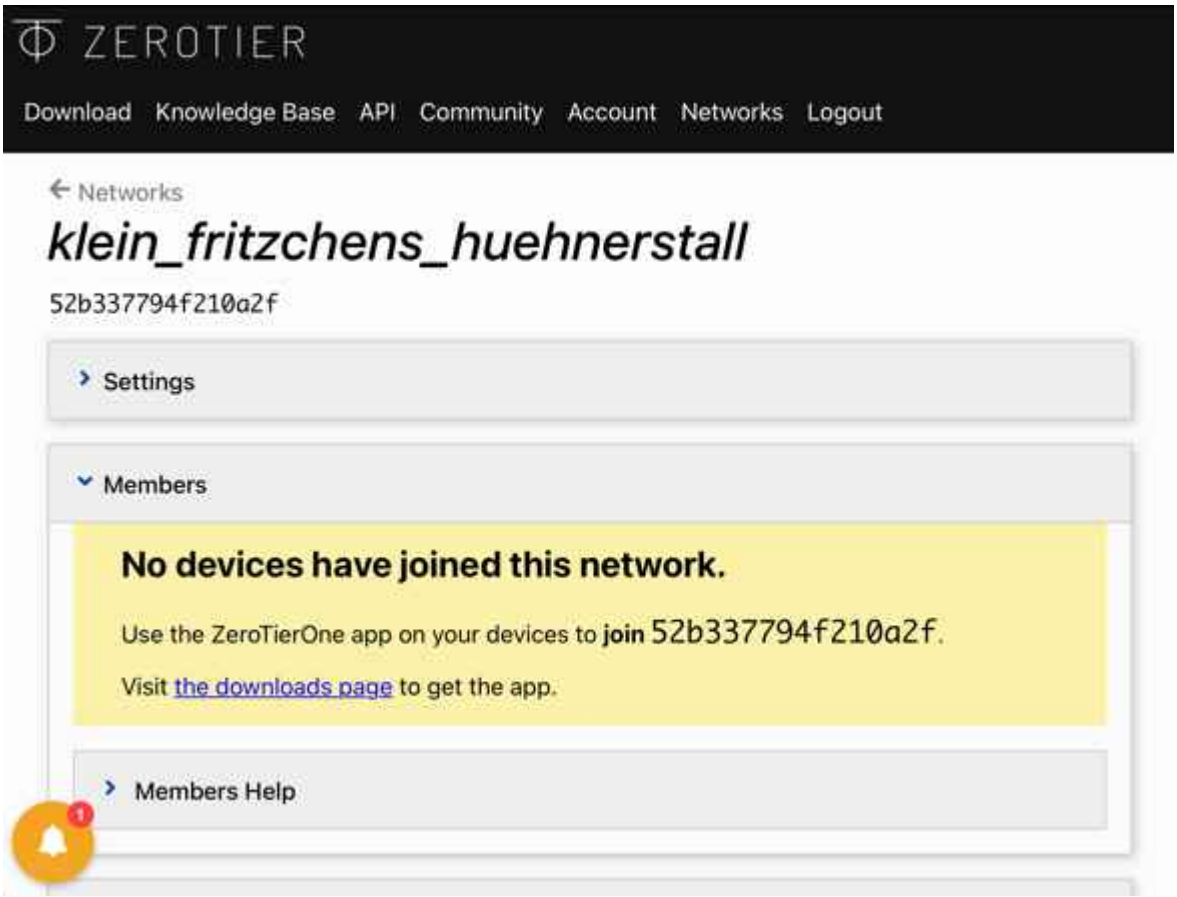
Auf der Beliebtheitsskala rangiert vor OpenVPN inzwischen das 2019 erschienene, ebenfalls quelloffene WireGuard, das auch schneller ist als OpenVPN & Co. Anders als OpenVPN und andere VPN-Verfahren klammert WireGuard die Benutzerverwaltung komplett aus und regelt nur die Vernetzung und das Chiffrieren von Nutzdaten mittels kryptografischer Schlüsselpaare. Wer sich für Implementierungsdetails interessiert, findet bei der Internet Engineering Task Force (IETF) eine Zusammenfassung für gängige VPNs, darunter TLS, IPsec und WireGuard (ct.de/y9y1). Beispiele für interessante, aber wenig verbreitete VPN-Varianten sind Nebula, SoftEther, Tinc, Twingate oder auch tinyfecVPN (dank spezieller Fehlerkorrektur empfehlenswert für gestörte Leitungen).

Netzwerkkopplung mit Komfort

Wer einfach nur von unterwegs auf einen Server im Heimnetz zugreifen will, den stellen die üblichen VPN-Anwendungen vor zu hohe Hürden. An diesem Punkt kommen VPN-Dienste ins Spiel, die man mittels vereinfachter Programme im Handumdrehen

verwenden kann. Zu den ersten Vertretern gehört das kostenpflichtige LogMeIn Hamachi, das sich nach dem Start über die Firewall des Heimrouters hinweg bei der Infrastruktur des Anbieters anmeldet. Anschließend können Hamachi-Clients laut dem Hersteller direkt miteinander kommunizieren (automatisches NAT-Traversal), also ohne den Umweg über Hamachi-Server. Bisher hat der Hersteller den Quellcode aber nicht veröffentlicht, sodass man weder die Sicherheit noch die Funktionsweise prüfen kann.

Zu den komfortablen, aber quelloffenen und geprüften VPNs gehören der WireGuard-Abkömmling Tailscale und ZeroTier. Mit ZeroTier verknüpft man Netzwerkgeräte über einen virtuellen Managed Switch, den ZeroTier anbietet (den man mit Abstrichen aber auch selbst betreiben kann) und der einfach per Web-Interface konfiguriert wird.



Als ZeroTier-Admin koppelt man PCs oder Smartphones innerhalb von Minuten in ein virtuelles Netzwerk. Wer den Dienst ausprobieren möchte, kann gratis eine Handvoll Netzwerke aufsetzen und Clients nach Belieben hinzufügen und entfernen.

Fortgeschrittene können ZeroTier-Gateways einrichten, die zwischen einem virtuellen Netz und einem physischen vermitteln.
Auf Linux, macOS, Windows, Android und iOS klappt das Einrichten mit geringem Aufwand, für den Verbindungsaufbau der Clients muss der UDP-Port 9993 geöffnet sein (alternativ UPnP für die beteiligten Hosts im Router einschalten). Das Web-Interface bietet zahlreiche Optionen, die sich an fortgeschrittene Admins richten. Beispielsweise kann man Subnetze beinahe nach Belieben wählen, öffentliche oder private Netze bilden, Netzwerkteilnehmern mehr als eine IP-Adresse und spezielle DNS-Resolver zuweisen oder Clients per Hand aus dem Netz kicken. ZeroTier ist quelloffen und von Fachleuten geprüft und für sicher befunden.

Stille VPNs

VPN-Funktionen verstecken sich manchmal an ungewöhnlichen Stellen. Das ist beispielsweise der Fall bei hybriden Internet-Anschlüssen. Dabei fasst ein Router im Zusammenspiel mit einem Hub im Rechenzentrum per VPN mehrere Internet-Leitungen zu einem Bündel zusammen, was die summierte Datenrate erhöht und die Ausfallsicherheit verbessert. Die Deutsche Telekom bietet solche Anschlüsse unter dem Namen „Magenta zu Hause Hybrid“ an. Dabei wird je ein DSL- und ein Mobilfunk-Zugang gebündelt. Der Router-Hersteller Viprinet bündelt beliebige Internet-Zugänge, ob DSL, Glasfaser, Kabel oder Mobilfunk.

Eine berüchtigte Gruppe unter den VPN-Anwendungen bilden Programme für das Peer-to-Peer-File-Sharing. Dabei versteckt die Sicherungsschicht die Nutzdaten. Manche Anwender verbreiten über diese Softwareklasse, die Napster begründet hat, illegal Medien und Programme. Das Piraten-Image haftet zwar weiter an, aber über Anwendungen wie BitTorrent werden etwa Linux-Distributionen weltweit kostengünstig verteilt und Unternehmen wie Microsoft nutzen die Technik, um Updates oder Spiele-Elemente zu verbreiten (z. B. beim Online-Rollenspiel

Skyforge).

Umgehung per Tunnel

Mit Aufkommen der Videostreamingangebote teilten vor allem US-amerikanische Medienhäuser den Weltmarkt in Regionen auf, um ihre Kommerzialisierungsideen durchzusetzen. Dafür werten deren Server den Standort der Nutzer aus: Wer aus einem noch nicht bedienten Gebiet anfragt, bekommt nichts zu sehen (Geoblocking). Filterkriterien sind beispielsweise die IP-Adressen der Nutzer und der Standort des befragten DNS-Resolvers, der den Anwendern beim Verbindungsaufbau die IP-Adresse der Streamingserver mitteilt. So bleiben etwa die Tore von HBO geschlossen, wenn man sich aus Europa anmeldet.

Mit VPN-Anwendungen täuscht man legitime Standorte vor, indem man den fernen Tunnelendpunkt in ein Land legt, das der Streaminganbieter versorgen will, also etwa in die USA. Ein derartiges VPN kann man mit etwas Know-how selbst basteln, indem man den VPN-Server in einer Cloud installiert, vorausgesetzt, man kann dessen Standort wählen. Solche Angebote kosten bei Amazon oder DigitalOcean monatlich wenige Euro. Zusätzlich muss das Betriebssystem des Nutzers einen Resolver aus dem Zielland befragen, sodass man auch diesen auf dem Cloudserver einrichtet oder einen offenen Resolver ausfindig macht, der im Zielland steht.

Privatsphärenschutz

Für jedes ferne Tunnelende braucht man aber einen separaten Server, sodass es schnell teuer wird, wenn man mehrere Endpunkte braucht. Deshalb, und auch weil die VPN-Konfiguration nicht jedermanns Sache ist, kamen vor einigen Jahren VPN-Anbieter auf den Markt, die genau dieses Anwendungsfeld mit eigenen Clients abdecken. Darüber kann man vor jedem Verbindungsaufbau einen von meist vielen Tunnelendpunkten per Menü auswählen.

Zusätzlich versprechen die Diensteanbieter, die Privatsphäre zu schützen, denn ohne VPN können Angreifer oder Spione Metadaten wie Ziel-Domains, Quell- und Ziel-IP-Adressen und unverschlüsselten Verkehr zum Beispiel an WLAN-Hotspots abfischen. Staatliche Sicherheitsorgane können solche Daten auch an Internet-Austauschknoten abgreifen.

Ein VPN schützt die Meta- und Nutzdaten kryptografisch, solange die Daten vom Nutzer zum Tunnelendpunkt unterwegs sind. Die VPN-Clients leiten daher sämtlichen Verkehr über den Tunnel zum VPN-Anbieter, der sie mit seiner eigenen Quell-IP-Adresse zum Ziel ins Internet gibt. Außerhalb des Tunnels erscheint nur die IP-Adresse des VPN-Anbieters. Deshalb lassen sich viele Metadaten nicht mehr korrekt zuordnen, weshalb sie für Angreifer und fremde Sicherheitsorgane wertlos sind.

Das gilt aber nicht für den Betreiber des VPNs, denn er kann den austretenden Verkehr den Nutzern prinzipiell anhand von Tunnel-IDs zuordnen. Deshalb erfordert es großes Vertrauen, ein VPN-Angebot zu buchen. Viele kommerzielle VPN-Anbieter sichern in den AGB zu, die Benutzeraktivitäten nicht zu protokollieren. Aber Kunden können das nicht prüfen. Tatsächlich deutet einiges darauf hin, dass manche Anbieter nur vorgeben, die Privatsphäre zu schützen, sie aber eigentlich sogar aushöhlen.

Sumpfiges Ökosystem

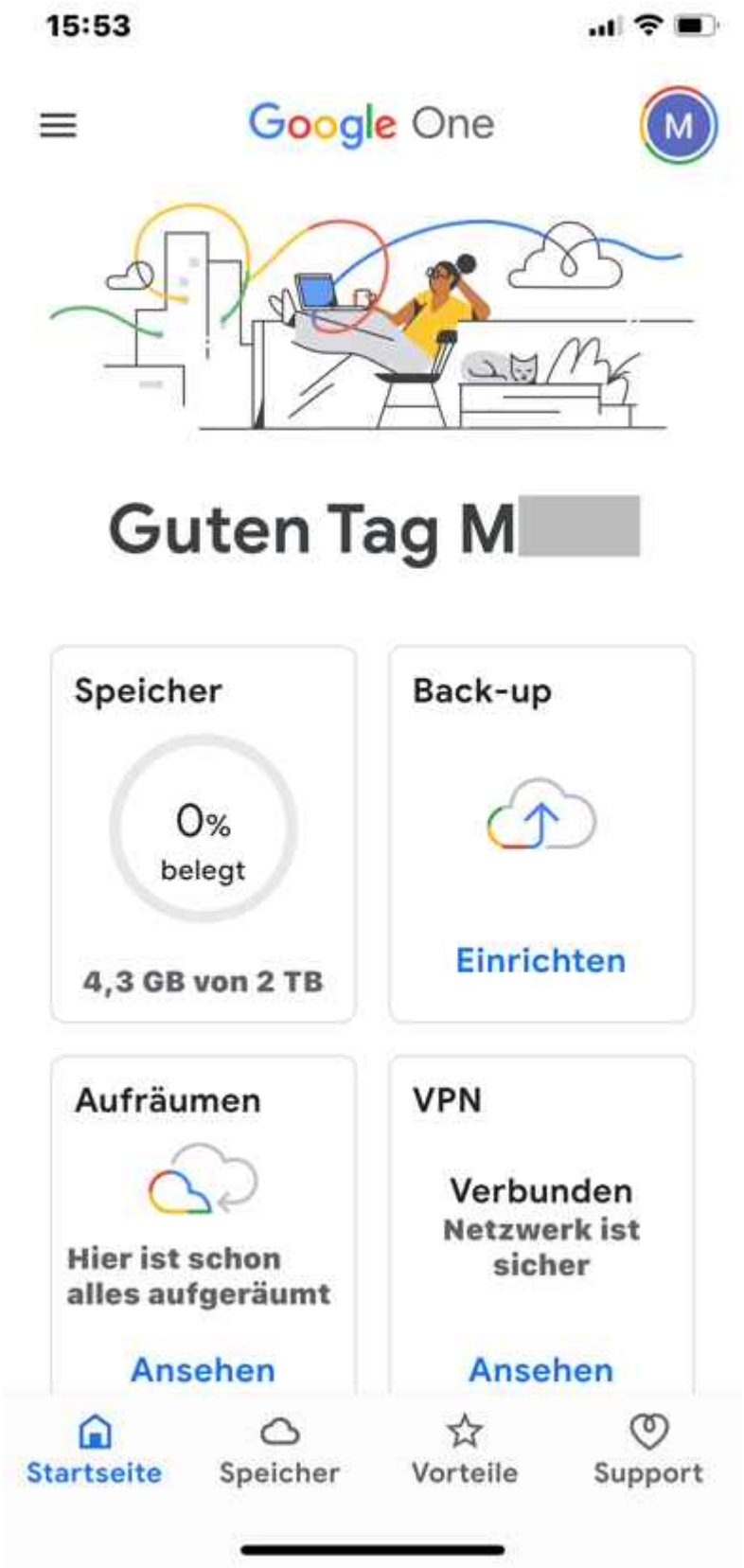
Beispielsweise deckte die Technologieforscherin und Redakteurin Katie Kasunic bereits im Juni 2020 auf, dass 40 VPN-Anbieter nach außen vorgeben, miteinander zu konkurrieren, tatsächlich aber der Kontrolle von nur sieben Unternehmen in Pakistan und China unterstehen. Beispielsweise kontrollierte zum Prüfzeitpunkt die in Singapur ansässige Firma Innovative Connecting insgesamt acht VPN-Anwendungen für Mobilgeräte, deren in China stationiertes Team entwickelte manche der Apps selbst und kontrollierte andere über stillschweigend aufgekaufte Tochterfirmen.

Solche Verflechtungen wecken Zweifel an der Vertrauenswürdigkeit von VPN-Anbietern. Auch erinnern die Firmenkonglomerate daran, dass in China vor einigen Jahren ungewöhnlich viele Tor-Exit-Punkte stationiert wurden. Das weckt den Verdacht, dass der oder die Betreiber am VPN- und Tor-Verkehr interessiert sind. Ein Exit-Node kann mitlesen und weiß lediglich nicht, wer die Daten anfordert. Es ist aber sichtbar, ob Tor-Nutzer zum Beispiel Webseiten abrufen, die einem autoritären Regime unliebsam sind. Auch der Opera-Browser, den manche Nutzer wegen seines eingebauten VPN-Verfahrens schätzen, segelt unter einer fragwürdigen Flagge: Dahinter steht ein Konsortium namens Golden Brick Silk Road Equity Investment Fund, das neben seinem Hauptsitz in China ein Büro in Russland unterhält.

Anscheinend haben also manche restriktiven Regierungen den Spieß umgedreht und nutzen VPNs offensiv zum Bespitzeln ihrer Nutzer. Dabei finanzieren die Bespitzelten durch den Kauf ihre Überwachung unwissentlich selbst.

Großer Entflechtungstrick

Unabhängig von ihrer Redlichkeit haben VPN-Anbieter ein strukturelles Problem: Kundendatenbanken und Verkehrsprotokolle können leicht miteinander verknüpft werden, um auszukundschaften, welche Ziele die VPN-Nutzer im Internet ansteuern. Selbst wenn ein Anbieter keine Log-Funktion eingerichtet hat, könnte er auf staatliche Weisung dazu gezwungen werden, womit die Privatsphäre der User perdu wäre.



Google hat eine eigene VPN-Anwendung für den Privatsphärenschutz entwickelt. Kundendaten und Kundenverkehr sind mittels moderner Kryptografietechniken entflochten.

An dieser Stelle greifen neue Angebote von Apple und Google. Beide entflechten die Authentifizierung der Anwender von den

Verkehrsdaten, sodass sich Benutzernamen und Einwahlzeitpunkte nicht mit IP-Adressen und durchgeleitetem VPN-Verkehr verknüpfen lassen. Dafür setzen beide Konzerne auf RSA Blind Signatures.

Die Technik erlangte in digitalen Wahlmaschinen einige Bekanntheit, weil sich damit digitale Wahlzettel so beglaubigen lassen, dass man die Inhalte keinem Wähler zuordnen kann. Eine Variante der Methode spezifizieren Apple, Cloudflare und Fastly unter dem Dach der Internet Engineering Task Force (siehe ct.de/y9y1).

Google verwendet RSA Blind Signatures beim kostenpflichtigen Dienst „Google One“. Der ist ab monatlich 10 Euro für macOS-, Windows-, Android- und iOS-Clients erhältlich; mit aktuellen Geräten der Pixel-7-Reihe soll der Dienst ab Dezember kostenlos sein. Der Client lenkt den gesamten Verkehr des Smartphones automatisch zum nächstgelegenen Tunnelendpunkt von Google, eignet sich also nicht zur Umgehung von Geoblocking.

Netzwerkverkehr einschließlich DNS, IP-Adressen und Verbindungszeiten werden Google zufolge nicht protokolliert, was den Dienst attraktiv erscheinen lässt. Wie bei anderen VPNs können auch hier Dritte im Datenstrom schnüffeln, sobald er den Tunnel verlassen hat, sodass man darauf achten muss, keine unverschlüsselten Anwendungen zu verwenden.

Die VPN-Varianten für Windows und macOS sind noch sehr frisch. Auf Android und iOS haben wir den Dienst ausgiebig getestet und dabei fielen nur wenige Fehlversuche auf. Der VPN-Client baut den Tunnel (vermutlich für Stromsparzwecke) häufig ab und bei Bedarf wieder auf und meldet jeden Statuswechsel. Wer das lästig findet, kann das Meldungsfeuer abschalten. Doch ob Sie ausgerechnet der Datenkrake Google auch noch fürs VPN vertrauen sollten, sei dahingestellt.

Apples Privatsphärenschutz Private Relay gibt es als Dreingabe zu einem iCloud+-Abo ab 0,99 Euro monatlich. Der Dienst setzt

iOS, iPadOS oder macOS voraus, ist aber ab Werk löchrig: Apple schützt mit Private Relay nicht den gesamten Verkehr des Nutzers, sondern nur den der eigenen Internet-Anwendungen. Dazu gehören DNS-Anfragen und der Verkehr des Safari-Browsers. Statt eines herkömmlichen VPN-Tunnels setzt Apple zwei verkettete Proxies ein (Multi-hop Masque proxy), die unterschiedlichen Betreibern gehören.

Der erste Proxy bekommt verschlüsselte Pakete und weiß daher nicht, welche Domain der Client ansteuern will. Nur der zweite kann sie entschlüsseln und leitet sie zum Ziel weiter, aber er weiß nicht, von welcher Quell-IP-Adresse die Pakete stammen. Deshalb weiß auch ein Webseiten-Betreiber nicht, welche IP-Adresse ein Besucher tatsächlich nutzt. Den ersten Proxy betreibt Apple selbst. Der zweite stammt aus einem Pool, den die CDN-Anbieter Akamai, Cloudflare und Fastly beisteuern. Aus diesem Pool stammen die IP-Adressen, die beim Surfen im Internet sichtbar werden (Test via ct.de/ip). Schaltet man einen VPN-Dienst ein, endet die Umleitung über die Proxies und der Verkehr läuft über den neuen Tunnel.

Wenn Private Relay eine DNS-Anfrage nicht auflösen kann, delegiert es die Aufgabe an den im Betriebssystem konfigurierten Resolver. Auf speziell konstruierten Webseiten wie astrill.com/dns-leak-test sickert so die IP-Adresse des Resolvers durch. Falls das einer ist, der auf Ihren Aufenthaltsort schließen lässt (etwa, weil sie zu Hause einen eigenen betreiben), richten Sie besser den anonymisierenden DNSCrypt-Proxy auf dem Mac ein (siehe ct.de/y46t); der ist auch für Windows und Linux empfehlenswert.

Trotz der Proxy-Kette wirkte Apples Dienst im Test schnell, Verzögerungen im Webseitenaufbau fielen gegenüber dem Betrieb ohne Private Relay nicht auf. Das dürfte daran liegen, dass die Proxies in CDNs stehen, die ohnehin viele nachgefragte Inhalte ausliefern. Im rund sechsmonatigem Test fiel Private Relay nur wenige Male aus und das auch nur vorübergehend. Einige wenige Webseiten, darunter HUK24.de, haben die Proxy-

IP-Adressen fälschlich dem europäischen Ausland zugeordnet und die Anmeldung abgelehnt. Nach Rückmeldungen der Nutzer beseitigten sie das Problem.

Verschleiernde VPNs

Große Firewalls können Datenpakete von gängigen VPNs einschließlich Google One leicht identifizieren und sperren. Auf dieser Grundlage setzen manche Staaten Internet-Zensur durch. Dem stellt eine große Entwicklergruppe das Tor-VPN entgegen. Es verschlüsselt und anonymisiert den Datenverkehr und verschleiert den VPN-Charakter, sodass die Datenpakete beispielsweise wie harmloser HTTP-Verkehr aussehen.

Tor ist hinlänglich bekannt und auch über dessen Snowflake-Erweiterung für Browser, die Tor-Clients zum Weg ins unzensierte Internet verhilft, haben wir berichtet (ct.de/y9y1). Aber da die Datenpakete über mehrere Vermittler ins Internet gelangen, sind sie viel länger unterwegs. Die Tor-Vermittler und der Endpunkt werden zufällig ausgewählt, sodass sich kaum rückverfolgen lässt, von wem eine Internet-Sitzung gestartet wurde. Aber manche restriktiven Regierungen betreiben eigene Tor-Endpunkte und können so mitlesen, welche Seiten im Web aufgerufen werden und Tor-Verkehr manipulieren.

An dieser Stelle kommt das VPN-Mauerblümchen Shadowsocks ins Spiel, das mutmaßlich einer Tastatur in China entstammt. Nachdem der Entwickler 2015 die Arbeit daran aufgeben musste, führten das Projekt andere fort und entwickelten Varianten. Unter diesen sticht das von Googles Jigsaw-Gruppe geführte Projekt Outline hervor. Shadowsocks und Outline standen jahrelang im Schatten von Tor, rückten aber kürzlich durch Netzsperren im Iran in den Blickpunkt.

Shadowsocks

Mit Shadowsocks kann man den Tunnelendpunkt selbst bestimmen, also sicherstellen, dass man keinen unerwünschten Tor-Endpunkt

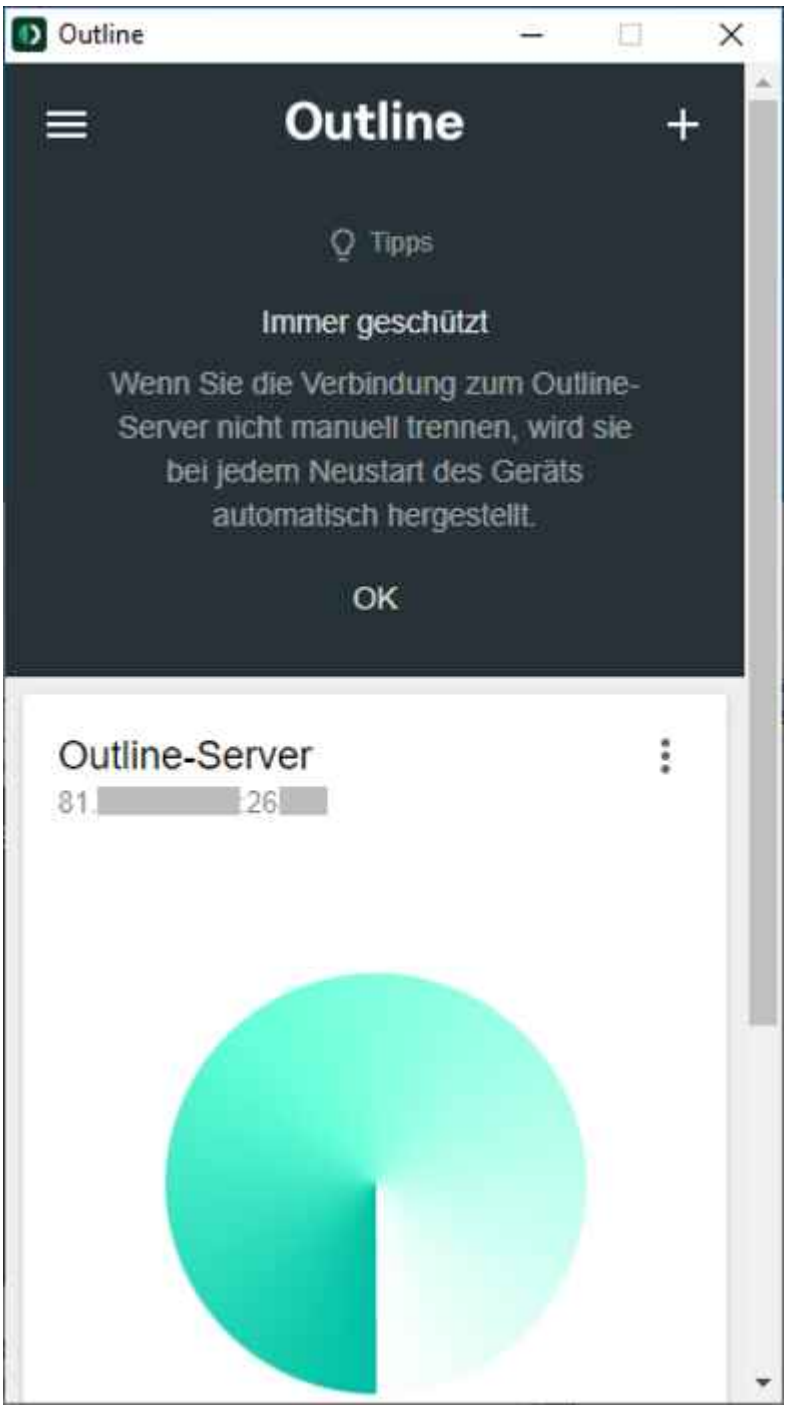
nutzt. Das scheint zwar die Anonymisierung auszuhebeln, weil man für den Server-Betrieb Cloud-Instanzen etwa bei Hetzner anmietet und dabei natürlich Personalien hinterlässt.

Aber manche Betreiber stellen ihre Shadowsocks-Server Nutzern aus dem Iran oder China auf Zuruf incognito und gratis zur Verfügung. Um dann unzensiert zu surfen, braucht man nur den Shadowsocks-Client und den zum Server passenden Schlüssel, der keinen Bezug zum Nutzer hat. Server lassen sich so konfigurieren, dass sie für alle Nutzer denselben Zugangsschlüssel verwenden. Unterm Strich können Betreiber selbst dann die Identität der Anwender nicht preisgeben, wenn ihr Server in fremde Hände fällt.

Mit Shadowsocks verbindet sich ein Client mit einem fernen SOCKS5-Proxy. Die Technik ähnelt dem Ansatz von SSH-Tunneln und wird auch bei Tor genutzt. Ist die Verbindung aufgebaut, leitet der Proxy den zu ihm gelangenden TCP- und UDP-Verkehr ins Internet.

Im Outline-Pelz

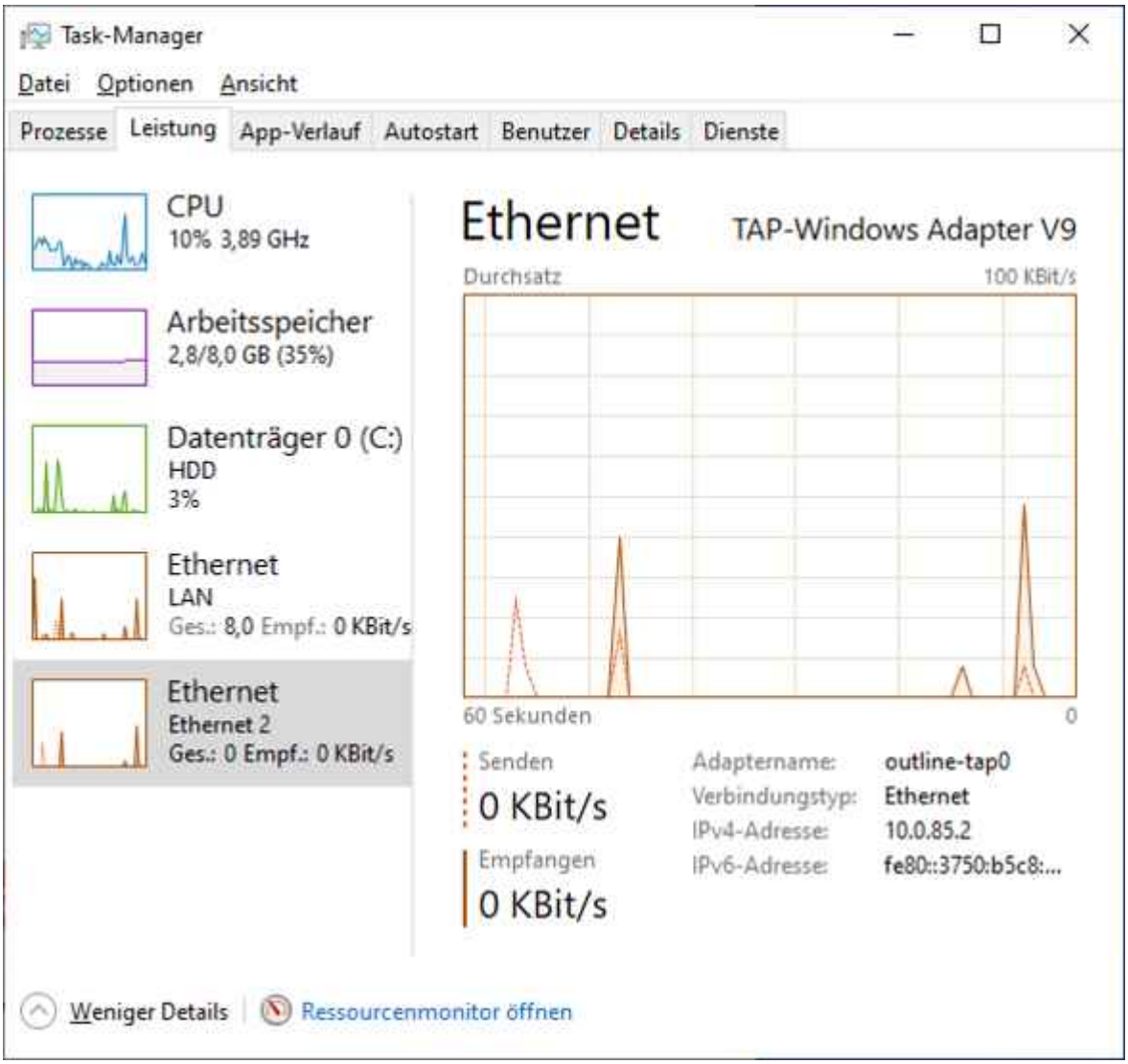
Die Jigsaw-Entwickler haben um Shadowsocks herum unter dem Namen Outline drei Anwendungen mit sehr übersichtlichen grafischen Oberflächen gebaut: Client, Server und Server-Manager. Alle drei sind für Linux, macOS und Windows erhältlich, die Clients auch für Android und iOS.



Von Googles Entwicklergruppe Jigsaw stammt auch die Shadowsocks-Variante Outline. Beide, Shadowsocks und Outline, verschleiern die Nutzdaten, um Firewallsperren zu entgehen.
Den Server installiert man mit dem Outline Manager typischerweise auf Cloud-Instanzen innerhalb von Minuten. Drei vereinfachte Installationen für DigitalOcean, Google und Amazon LightSail bietet der Manager gleich auf seiner Startseite an. Aber für das Einrichten auf anderen Linux-Servern oder im Firmennetz braucht man ebenso wenig Vorkenntnisse, denn die Installationsskripte erledigen den Großteil selbst.

Die Jigsaw-Entwickler bieten Outline hauptsächlich für Nachrichtenagenturen und Journalisten an, die aus Ländern mit Internet-Sperren berichten. Outline ist wie Shadowsocks quelloffen und gilt als sicher und vertrauenswürdig; es wurde 2017 und 2018 von Spezialisten auf Herz und Nieren geprüft. Allerdings lässt es sich einem Bericht zufolge trotz Verschleierungstechniken mit etwas Aufwand identifizieren (siehe ct.de/y9y1).

Deshalb lässt sich der Zugriff auf Outline-Server sperren. Das erfolgt allerdings per Hand und krude anhand von Ziel-IP-Adressen, weshalb sich Outline-Sperrungen nur dann häufen, wenn sich die politische Lage zuspitzt. Als Gegenmaßnahmen empfehlen die Outline-Entwickler den Betrieb mit mehreren IP-Adressen unter demselben Domainnamen (ct.de/y9y1).



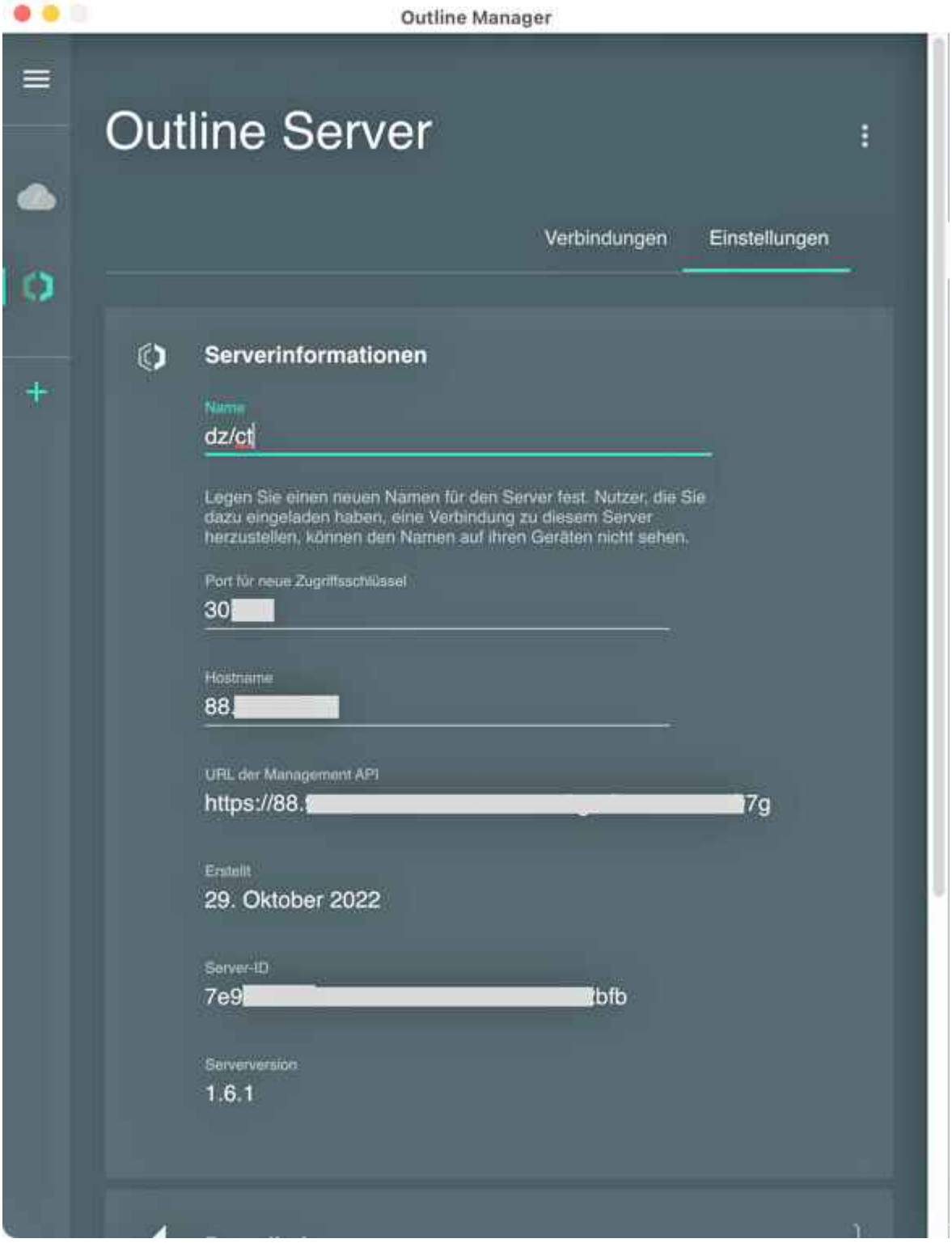
Der Outline-Client installiert auf Windows ein virtuelles TAP-

Interface und lenkt darüber allen ausgehenden Internet-Verkehr in den Tunnel zum Outline-Server.

Outline Manager und Server

Ausgehend vom Outline Manager haben wir den Outline-Server auf zwei Debian-VMs installiert, es klappte auf beiden im Nu und reibungslos. Dabei nimmt ein Bash-Skript dem Admin sehr vieles ab; es verlangt nur einige wenige Angaben. Am Ende fällt ein URL heraus, den man in den Outline-Manager kopiert und ein Zugangsschlüssel mitsamt Server-URL, die man an die Nutzer verteilt.

Darüber hinaus bietet der Manager nur wenige weitere Funktionen. Man kann für Clients Obergrenzen für das Übertragungsvolumen festlegen und Verwaltungsdaten wie IP-Adresse oder Server-ID ablesen – das wars auch schon. Infos und diverse Statistiken liefert das Monitoring-Tool Prometheus, das man auf dem Outline-Server über die lokale IP-Adresse 127.0.0.1 und die TCP-Ports 9090, 9091 und 9092 anzapft. Außerdem bietet Google einen Metrics-Server auf Grundlage der Google App Engine; er setzt Googles Cloud SDK voraus (ct.de/y9y1).



Das Einrichten des Outline-Servers startet man auf Linux, macOS oder Windows mit dem Outline Manager. Anschließend läuft auf dem Zielserver ein Bash-Skript und richtet dort einen Docker-Container mit Shadowsocks ein – was alles ohne besondere Netzwerkkenntnisse klappt.

Prinzipiell sollte der Server auch auf anderen Betriebssystemen laufen, denn er steckt in einem Docker-Container auf Basis der Alpine-Distribution 3.11.6 (siehe

Docker-Plattform Quay, ct.de/y9y1). Das Installationsskript des Outline Managers sieht aber nur Linux-Plattformen (x86_64) als Zielserver vor.

Um zu prüfen, was das Skript tut, lädt man es einfach aus dem GitHub-Projekt von Jigsaw (siehe ct.de/y9y1) auf einen PC und liest es in einem Editor. Unter anderem installiert es Docker, falls das fehlt, und richtet den Container mitsamt dem Zugriffsschlüssel ein.

Insgesamt liefen beide Server-Instanzen im mehrwöchigen Testbetrieb reibungslos. Zwar haben die Entwickler den Container seit zwei Jahren nicht aktualisiert, sodass die automatische Test-Routine von Quay viele und auch kritische Sicherheitslücken meldet. Sie betreffen aber nur den Befehl curl 7.67.0 (Release-Datum 6.11.2019), den man im Serverbetrieb nicht nutzt. Wer die Lücken trotzdem eliminieren will, findet die erforderlichen Update-Befehle im Quay-Repository (siehe ct.de/y9y1).

Outline Client

Der Outline Client ist ebenfalls flink installiert. Hat man ihm eine passende URL spendiert, baut er die Verbindung zum Server umgehend auf und signalisiert das im Menü. Fortan läuft jeglicher Internet-Verkehr durch den Tunnel. Auf Macs kann man das beispielsweise mit dem Befehl netstat -rn | grep 'default' auslesen. Dabei wird sichtbar: Der gesamte Verkehr wird an ein virtuelles TUN-Interface geleitet (z. B. utun10).

Mit ifconfig utun10 kann man die (lokale) Ziel-IP-Adresse auslesen (inet 169.254.19.0) und route -n get <domain> zeigt, über welchen Weg ein bestimmtes Ziel angesprochen wird:

route -n get ct.de

gibt zum Beispiel Folgendes aus:

route to: 193.99.144.80

```
destination: default
interface: utun10
```

Wer im Container herumspaziert, findet bald, dass die Jigsaw-Entwickler zur DNS-Auflösung der VPN-Clients die DNS-Resolver von Google konfiguriert haben. So schenkt man Google die Surf-Ziele der VPN-Nutzer. Google sichert immerhin zu, dass es DNS-Anfragen anonymisiert und spätestens nach 48 Stunden löscht. Wer trotzdem andere Resolver will, muss den Container editieren und etwa 9.9.9.9 eintragen (Resolver des gemeinnützigen Anbieters Quad9).

Fazit

VPN-Funktionen bilden heute für sehr viele Anwendungen die Kommunikationsgrundlage, obwohl die Technik ursprünglich nur zur Vernetzung von Standorten gedacht war. Manche Anwendungen verändern sich (Peer-to-Peer für Filesharing) und manche greifen Methoden aus teils scheinbar fernen Bereichen auf, etwa die Nutzdatenverschleierung bei Shadowsocks oder die RSA Blind Signatures beim Privatsphärenschutz von Apple und Google.

Das liegt in der Natur der Sache, denn die VPN-Entwicklung unterliegt einem starken Optimierungsdruck. Auf weitere Innovationen kann man ebenso gespannt sein wie darauf, ob und welche weiteren VPN-Anbieter diese aufgreifen. *(dz@ct.de)*

VPN-Infos: ct.de/y9y1

WordPress – Plugins

Ausbaumodule

Eine der größten Stärken von WordPress sind seine zahlreichen Plug-ins. Die große Entwicklergemeinde des Content-Management-Systems hat rund 60.000 solcher Erweiterungen hervorgebracht. Dieser Artikel stellt eine Auswahl der wichtigsten vor, mit denen Sie WordPress für fast jeden Einsatzzweck ausrüs…

WordPress mit Plug-ins erweitern

Eine der größten Stärken von WordPress sind seine zahlreichen Plug-ins. Die große Entwicklergemeinde des Content-Management-Systems hat rund 60.000 solcher Erweiterungen hervorgebracht. Dieser Artikel stellt eine Auswahl der wichtigsten vor, mit denen Sie WordPress für fast jeden Einsatzzweck ausrüsten.

Von Jo Bager und Daniel Berger

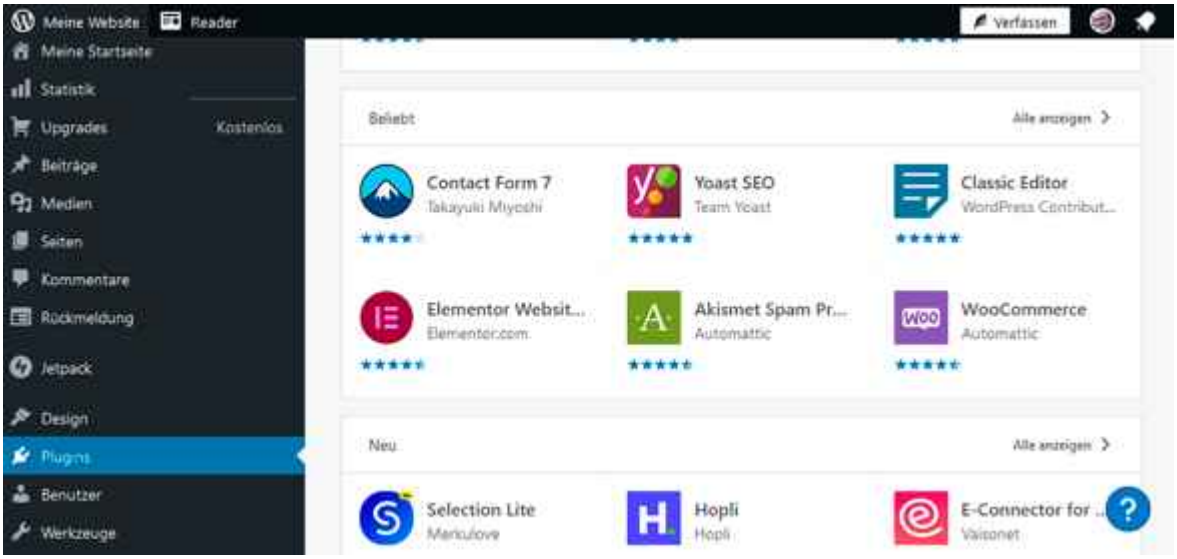
Plug-ins bohren WordPress’ Funktionen auf: Sie rüsten schicke Bildergalerien nach, stellen sicher, dass Seiten gut bei

Google ranken und können sogar komplette Shops nachrüsten. Die Erweiterungen lassen sich mit ein paar Klicks einrichten. Einen Katalog der Plug-ins finden Sie im WordPress-Backend unter „Plug-ins/Installieren“. Im Bereich „Vorgestellt“ empfehlen die WordPress-Macher einige Klassiker. Unter „Populär“ sind die momentan angesagten Plug-ins zu sehen. Ausgehend von bereits installierten Erweiterungen, zeigt WordPress unter „Empfehlungen“ weitere Vorschläge an. Über die Suchfunktion können Sie die gesamte Sammlung nach Schlüsselwörtern durchforsten und finden leicht auch die in diesem Artikel empfohlenen Erweiterungen.

Das Multitool

Statt eine Vielzahl von Plug-ins zu installieren, reicht oftmals schon **Jetpack** aus – eine Sammlung von Werkzeugen und Funktionen von den WordPress-Machern, die allerlei Bereiche abdecken: Das darin enthaltene Bilder-Karussell etwa setzt Fotos schick in Szene. Jetpack kann neue Posts automatisch bei sozialen Medien wie Facebook, Twitter und LinkedIn posten und das Plug-in schützt die Website vor Brute-Force-Angriffen, bei denen Angreifer versuchen, Zugangsdaten zu erraten und damit Ihre Site zu übernehmen.

Allerdings ist Jetpack eng mit dem WordPress-Hersteller Automattic verzahnt. Um Jetpack zu benutzen, ist ein kostenloser Account bei wordpress.com nötig, den Sie mit der eigenen WordPress-Installation verknüpfen. Einige Jetpack-Fähigkeiten kosten Geld, etwa der Spam-Schutz oder die automatische Backup-Funktion, die eine Website absichert. Zahlende Kunden bekommen außerdem „Priority Support“ via E-Mail. Die Preise beginnen bei rund 40 Euro im Jahr. Über manche der Funktionen von Jetpack können Daten an wordpress.com und letztlich auch an Fremdanbieter fließen. Wenn Sie das Plug-in nutzen, müssen Sie daher Ihre Datenschutzerklärung entsprechend ergänzen.



Plug-ins lassen sich bequem aus dem Backend heraus suchen und installieren.

Alles sicher

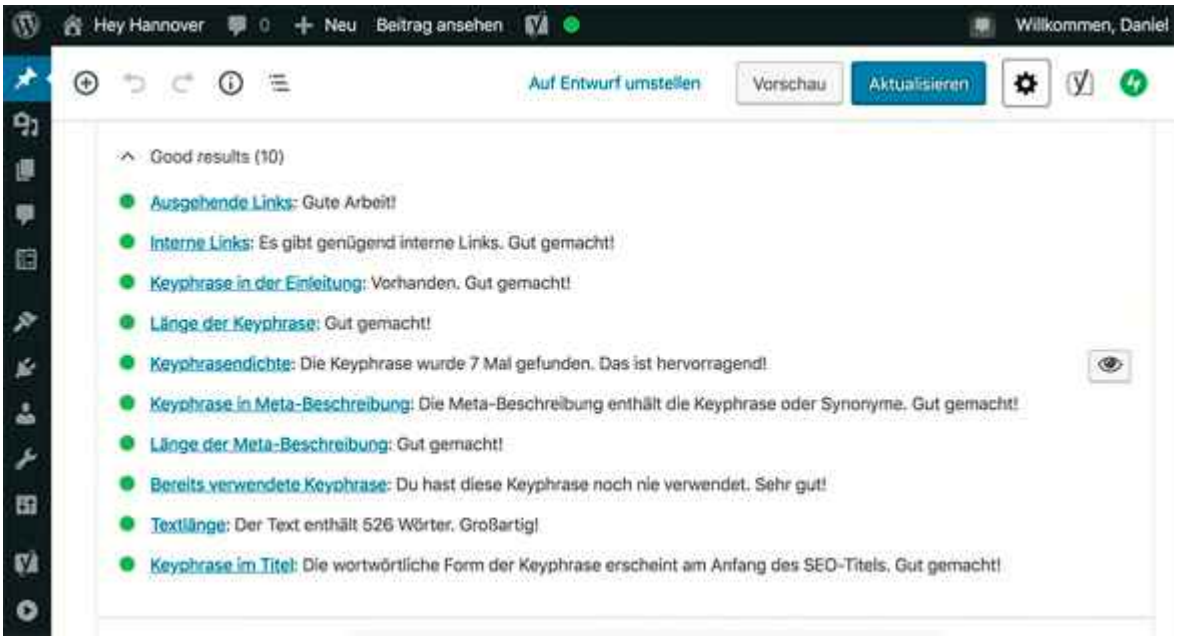
Wenn Sie Jetpack nicht nutzen möchten, sollten Sie Angreifer anderweitig daran hindern, massenhaft Zugangsdaten auszuprobieren, um sich Zugang zu Ihrer Website zu verschaffen. Das Plug-in **Limit Login Attempts Reloaded** ist eine gute Alternative, es begrenzt die Anzahl der möglichen Login-Versuche. Eine Zwei-Faktor-Authentifizierung sichert den Zugang zu WordPress zusätzlich: Um sich einzuloggen, ist neben dem Nutzernamen und dem Passwort ein individueller Code nötig. Den erzeugt zum Beispiel die Android- und iOS-App Google Authenticator. Auf Ihrer WordPress-Instanz müssen Sie eine passende Erweiterung installieren, etwa das ebenfalls **Google Authenticator** genannte Plug-in von Ivan Kruchkoff.

Auch Spammer lieben WordPress: Ihr Angriffsziel ist die Kommentarfunktion. **Antispam Bee** unterbindet solchen Kommentarspam. Im Unterschied zu ähnlichen Plug-ins kommt es ohne Cloud-Zugriffe aus, um Spam zu erkennen. Es gleicht Kommentare stattdessen mit einer lokalen Datenbank ab, was deutlich datenschutzfreundlicher ist.

Erster bei Google

Suchmaschinenoptimierung (Search Engine Optimization, SEO) ist nützlich, damit man Ihre Website per Suchmaschine besser findet und dadurch die Besucherzahlen steigen. Das populäre Plug-in **Yoast SEO** greift Ihnen dabei unter die Arme. Die Basisversion kostet nichts und reicht für die meisten Websites.

Die Erweiterung klinkt sich in die Beitragsseite von WordPress ein, analysiert Ihre Texte und gibt hilfreiche Verbesserungstipps. Das Plug-in bemängelt beispielsweise zu kurze Beiträge (Google liebt lange Texte) und fehlende Zwischenüberschriften in längeren Beiträgen. Außerdem können Sie mit Yoast SEO sinnvolle Metadaten festlegen und die Überschrift optimieren. Sie taucht samt Meta-Description bei Google in den Suchergebnissen auf.



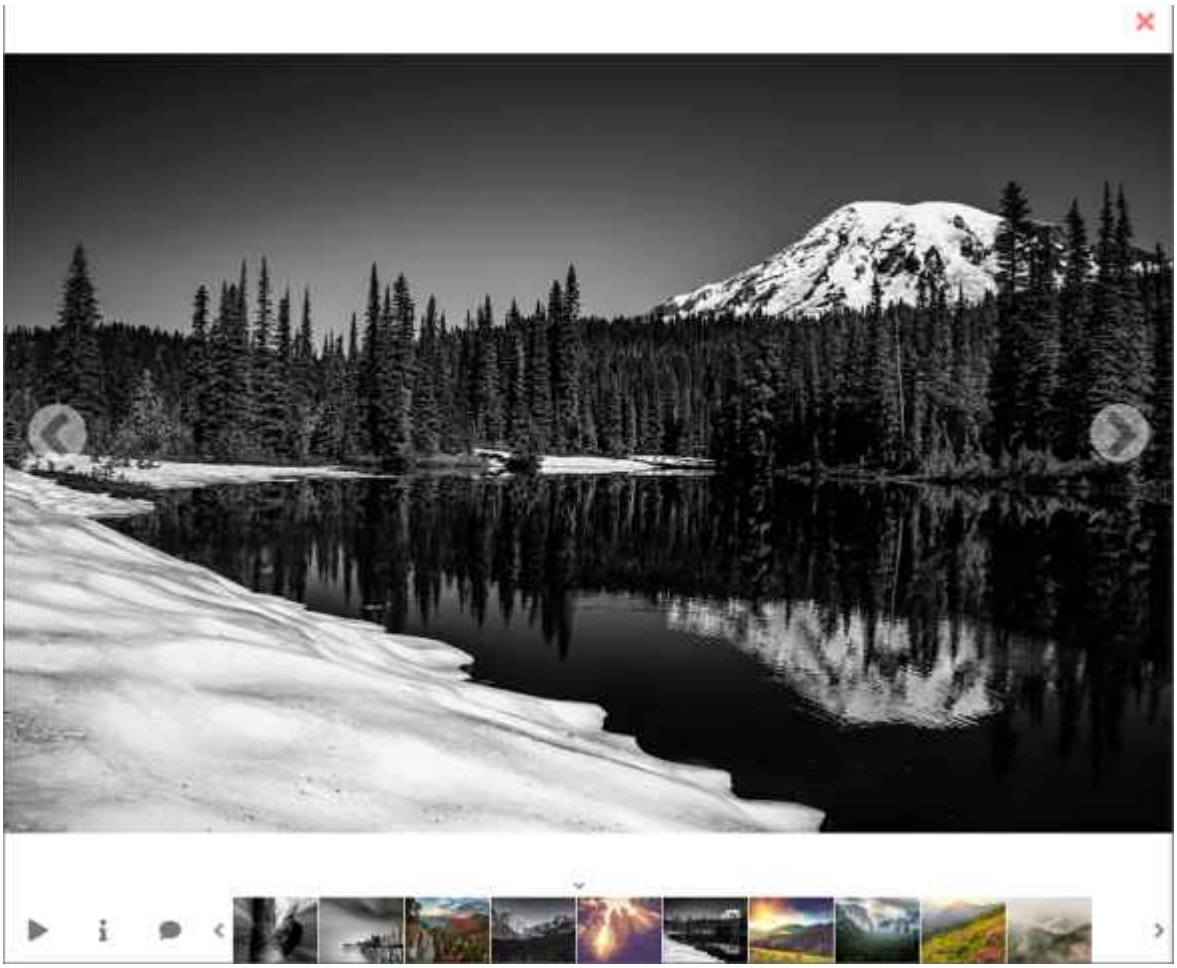
Alles suchmaschinentauglich? Yoast SEO untersucht Texte und Einstellungen der Website und gibt Verbesserungsvorschläge.

Bilder rahmen

WordPress hat zwar Funktionen zur Verwaltung und Präsentation von Bildern eingebaut (siehe S. 65), doch wer mit sehr vielen Bildern arbeitet, stößt schnell an die Grenzen der Bordmittel.

Mit **NextGEN Gallery** können Sie Bilder im WordPress-Backend effizient organisieren und auf der Website gut in Szene setzen. Fotos lassen sich im Batchbetrieb hochladen und bearbeiten, Galerien in Alben gruppieren und vieles mehr.

NextGEN Gallery unterstützt bereits in der kostenlosen Version mehrere Galerie- und Albumstile, die sich alle in Bezug auf Größe, Stil, Timing, Übergänge, Steuerelemente und Lightbox-Effekte individualisieren lassen. Neben der kostenlosen Version des Plug-ins gibt es noch Bezahlversionen, unter anderem mit weiteren Stilen für Galerien und Alben.



NextGEN Gallery hilft bei der Organisation der Bilder im Backend und stellt auch schicke Galerien für die Präsentation bereit.

Mit Besuchern in Kontakt treten

Mit der Kommentarfunktion von WordPress können Besucher ihre Meinung zu einzelnen Beiträgen ausdrücken und miteinander

diskutieren. Aber vielleicht möchten Sie Ihren Lesern die Möglichkeit geben, sich unabhängig von einem Blogbeitrag direkt an Sie zu wenden? Dann hilft das kostenlose Plug-in **Contact Form 7**, mit dem Sie schnell ein schickes Kontaktformular zusammenklicken können. Das Plug-in ist in der Standardkonfiguration datenschutzfreundlich und verschickt die eingegebenen Daten lediglich an Sie per Mail. Contact Form 7 kann Ihre Formulare auch gegen Spam absichern. Dazu bettet es allerdings Funktionen von Dritten ein, zum Beispiel Google reCAPTCHAs oder Akismet vom WordPress-Hersteller Automattic.

Falls die Diskussionen Ihrer Leser die Kommentarfunktion sprengen, können Sie mit dem kostenlosen **bbPress** ein richtiges Diskussionsforum nachrüsten, mit Benutzerverwaltung und themenbezogenen Unterforen. Noch einen Schritt weiter geht **BuddyPress**. Mit diesem Plug-in können Sie eine Art soziales Netzwerk betreiben und Besuchern Ihrer Site erlauben, detaillierte öffentliche Mitgliederprofile zu unterhalten, Gruppen zu gründen, sich einander private Nachrichten zu senden und noch viel mehr.

Apropos soziale Medien: Wenn Sie auf Ihren WordPress-Seiten Inhalte von Facebook oder anderen Diensten einbetten, übertragen Sie Daten des Besuchers – mindestens die IP-Adresse – zu dem Anbieter, sobald der Benutzer die Seite abruft. Besser (und gesetzeskonform) ist es, wenn der Besucher selber entscheiden kann. Das stellen Sie mit dem **Shariff Wrapper** sicher.

Dabei handelt es sich um eine speziell für WordPress angepasste Version des c’t Shariffs. Die WordPress-Version unterstützt 32 Dienste in 25 Sprachen, darunter große Anbieter wie Facebook, Twitter und Paypal bis hin zu regionalen Diensten und Exoten wie Odnoklassniki und Diaspora.

Shop und PR

Mit WordPress lassen sich auch komplette Webshops betreiben.

Das Plug-in **WooCommerce** hat sich dafür als Quasi-Standard etabliert. Laut WordPress-Statistik nutzen über fünf Millionen aktive Installationen dieses Plug-in. Unter den 1.000.000 größten E-Commerce-Websites werden knapp 30 Prozent als Kombination von WordPress mit WooCommerce betrieben, haben die Web-Statistiker bei BuiltWith nachgezählt.

WooCommerce ist unter anderem deshalb so beliebt, weil es sich selbst wieder mit diversen Plug-ins für die verschiedensten Zwecke feintunen lässt. **Germanized für WooCommerce** zum Beispiel erweitert es um die Funktionen für den rechtssicheren Betrieb eines Shops in Deutschland. Es ergänzt Hinweise für Versandkosten und Steuern, Optionen zum Anhängen rechtlicher Hinweistexte wie die Widerrufsbelehrung an E-Mails und vieles mehr. Alles in allem ist WooCommerce sehr komplex. Sie finden auf heise+ einen eigenen Artikel zu Einrichtung und Betrieb eines Shops mit dem Plug-in [1].

Insbesondere wenn Sie über Ihre Website Dienstleistungen anbieten, sollten Sie verlässliche Kontaktmöglichkeiten bereitstellen. Der Kommunikation zwischen dem Website-Betreiber und seinen Besuchern hat sich **Tidio** verschrieben. Mit dem Plug-in können Sie einen Live-Chat einrichten. Ein Chatbot kann den Chat erweitern. Damit können Sie auch dann Besucher automatisiert „abholen“, wenn Sie persönlich gar nicht online sind.

Eine weitere Methode, um mit Nutzern zu kommunizieren, sind Newsletter. Sie erfreuen sich in letzter Zeit wieder enormer Beliebtheit [2]. Damit Sie sich voll auf Inhalte konzentrieren können, nimmt Ihnen das schlicht **Newsletter** getaufte Plug-in die Handarbeit ab. Es führt die Empfängerlisten, sorgt für einen kontrolliert langsamen Versand, damit der Newsletter nicht als Spam aussortiert wird, und führt Reporte, zum Beispiel über Öffnungsraten. Newsletter ist kostenlos und nach Angaben der Herausgeber DSGVO-konform.

Websites können Besucher auch direkt per Push-Notification

informieren. Bei WordPress-Sites lässt sich diese Funktion zum Beispiel mit dem Plug-in des Dienstleisters **OneSignal** nachrüsten. Bis zu 10.000 Empfänger sind kostenlos.

Egal ob Chatbot, Newsletter oder Push-Notification: Achten Sie darauf solche Möglichkeiten maßvoll und im Sinne Ihrer Nutzer einzusetzen. Man kann sich damit nämlich auch leicht unbeliebt machen.

Risiken und Nebenwirkungen

Falls Sie in unserer Auswahl nicht das benötigte Plug-in gefunden haben und deshalb das Verzeichnis von WordPress durchforsten: Achten Sie bei der Auswahl auf die Zeitangabe bei „Zuletzt aktualisiert“. Wenn es schon seit Langem kein Update mehr gab, blendet WordPress sicherheitshalber einen Warnhinweis ein. Die Zahl bei „Aktive Installationen“ verrät, wie populär eine Erweiterung ist. Lesen Sie zudem die Nutzerkommentare und checken die „durchschnittlichen Bewertungen“. Finden sich 1-Stern-Rezensionen, sollten Sie nach etwaigen Problemen Ausschau halten, die vielleicht erst seit Kurzem bestehen.

Der einfache Installationsprozess macht es reizvoll, schnell mal ein paar Dutzend dieser Erweiterungen zusammenzuklicken. Sie sollten es aber aus mehreren Gründen nicht übertreiben: Mit zu vielen Plug-ins droht die Performance Ihrer Website einzubrechen. Zudem können sich Plug-ins gegenseitig ins Gehege kommen. Sollte es plötzlich Probleme geben, schalten Sie die verdächtigen Plug-ins ab und nacheinander wieder ein, um den Störenfried zu finden.

Vor allem gehören (veraltete) Plug-ins zu den größten Einfallstoren für Schadcode und andere Attacken auf WordPress-Installationen. Achten Sie daher genau darauf, nur aktuelle Plug-ins einzusetzen und sortieren Sie aus, was Sie nicht mehr brauchen. Im Menü unter „Dashboard/Aktualisierungen“ können Sie schnell prüfen, ob alles auf dem neuesten Stand ist, und

nötige Plug-in-Aktualisierungen auch gleich anstoßen.

Dies ist die gekürzte und überarbeitete Version eines Artikels, der zuerst in Mac & i extra Workshops erschien. (jo@ct.de)

1. Literatur
2. Andreas Hitzig, WordPress-Plugin: Der eigene Online-Shop mit WooCommerce: https://heise.de/-4997674
3. Jo Bager, Kuratiert ins Postfach, Die Renaissance der Newsletter, c't 22/2020, S. 120

Plug-ins: ct.de/yc2d

WordPress – Themes

Mehr als eine schöne Hülle

Das Theme bestimmt nicht nur das Aussehen einer WordPress-Site, es beeinflusst auch ihren Funktionsumfang und ihre Struktur. Deshalb ist es wichtig, ein passendes Theme auszuwählen. Dieser Artikel zeigt, worauf Sie dabei achten müssen und präsentiert eine Auslese besonders vielseitiger und hübscher…

WordPress-Themes: Worauf kommt es an?

Das Theme bestimmt nicht nur das Aussehen einer WordPress-Site, es beeinflusst auch ihren Funktionsumfang und ihre Struktur. Deshalb ist es wichtig, ein passendes Theme auszuwählen. Dieser Artikel zeigt, worauf Sie dabei achten müssen und präsentiert eine Auslese besonders vielseitiger und hübscher Themes.

Von Vladimir Simović

Beim Aufziehen einer Website mit WordPress kommt fast unmittelbar nach der Installation die Frage auf, welches Theme zum Einsatz kommen soll. Ein späterer Wechsel ist meist mit umständlichen Anpassungen verbunden. Den damit einhergehenden Aufwand und die Kosten sollten Sie nicht unterschätzen. Umso wichtiger ist es, sich vorher Gedanken über das richtige Theme zu machen.

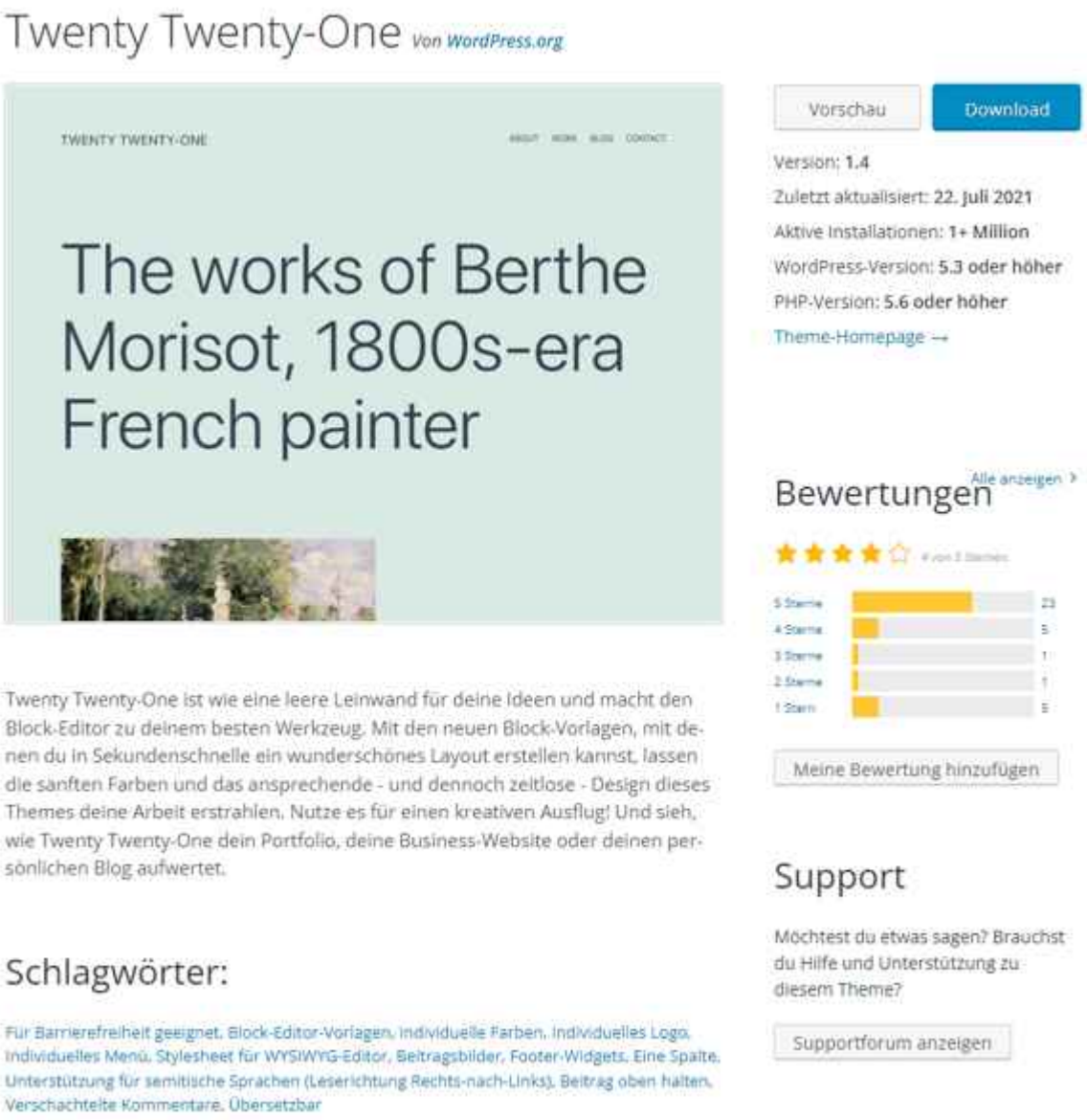
Ein Problem dabei ist, unter den Tausenden kostenlosen und kostenpflichtigen Themes ein passendes zu finden. Etliche werden in einem Freemium-Modell vertrieben: Eine Basis-Version kostet nichts; wer mehr will, muss in die Tasche greifen. Ihre kostenpflichtigen Themes vertreiben die Hersteller häufig mit mehreren Bezahlmodellen: Für einen einmaligen Betrag, bei hochwertigen Themes im dreistelligen Bereich, erwerben Sie ein lebenslanges Nutzungsrecht – mitunter für die Nutzung auf

mehreren Sites. Sie können Themes aber auch zu einem günstigeren Jahrestarif mieten.

Das offizielle Theme-Verzeichnis von WordPress erreichen Sie entweder direkt über das Backend Ihrer WordPress-Installation oder im Web unter wordpress.org/themes/. Es listet nur kostenfreie Themes und kommerzielle Themes, die unter einer Lizenz angeboten werden, die mit der GNU General Public License (GPL) kompatibel ist. Insgesamt finden sich dort knapp 9000 Themes. Andere Premium-Themes erhalten Sie entweder über die Websites der Entwickler direkt oder über spezialisierte Portale wie themeforest (siehe ct.de/y8ea).

Bevor Sie sich für ein bestimmtes Theme entscheiden, sollten Sie einige Eckpunkte prüfen:

- Wird es aktiv gepflegt? Wann war die letzte Aktualisierung?
- Gibt es Support oder eine Community, die bei Fragen helfen kann?
- Ist das Theme responsive, passt es sich also verschiedenen Displaygrößen und Gerätetypen automatisch an?
- Ist es darauf optimiert, dass die Inhalte in Suchmaschinen gut platziert werden (SEO)?
- Ist das Theme optimiert in Bezug auf die Ladezeit?



Der Steckbrief eines Themes im WordPress-Verzeichnis liefert viele aussage-kräftige Basisinformationen.
Antworten zu einigen dieser Fragen finden Sie auf der Seite eines Themes im WordPress-Verzeichnis. Dort stehen Informationen zu den Anforderungen, Bewertungen durch andere Nutzer sowie Links zum Code, dem Development Log und, falls vorhanden, zur externen Theme-Homepage beim Hersteller. Haben Sie ein Theme näher ins Auge gefasst, können Sie sich im Themes-Verzeichnis auch eine Vorschau ansehen. Sie sollten auch einen genauen Blick darauf werfen, welche Funktionen und Extras es bietet. Viele wichtige Auswahlkriterien finden Sie unter den „Schlagwörtern“ auf der Theme-Seite.

Diese Schlagwörter können Sie auch als Filter in der Suchfunktion einsetzen, um infrage kommende Themes zu finden.

Viele der Schlagwörter sind selbsterklärend: „Für Barrierefreiheit geeignet“, „Individuelle Farben“, „Individuelles Logo“, „Beitragsbilder“, „Footer-Widget“, „Beitrag oben halten“ et cetera.

„Übersetzbar“ heißt, dass sich das Theme auch für mehrsprachige Websites eignet. „Block-Editor-Vorlagen“ bedeutet, dass das Theme den Gutenberg-Editor (siehe S. 64) mit eigenen Vorlagen erweitert. Man kann auch nach Layout-Aspekten filtern, etwa nach der Anzahl der Spalten oder nach dem Vorhandensein einer linken oder rechten Seitenleiste. Außerdem können Sie nach der inhaltlichen Ausrichtung Ihrer Website filtern (Blog, Bildung, E-Commerce etc.).

Pagebuilder: Hilfsmittel und Problemquelle

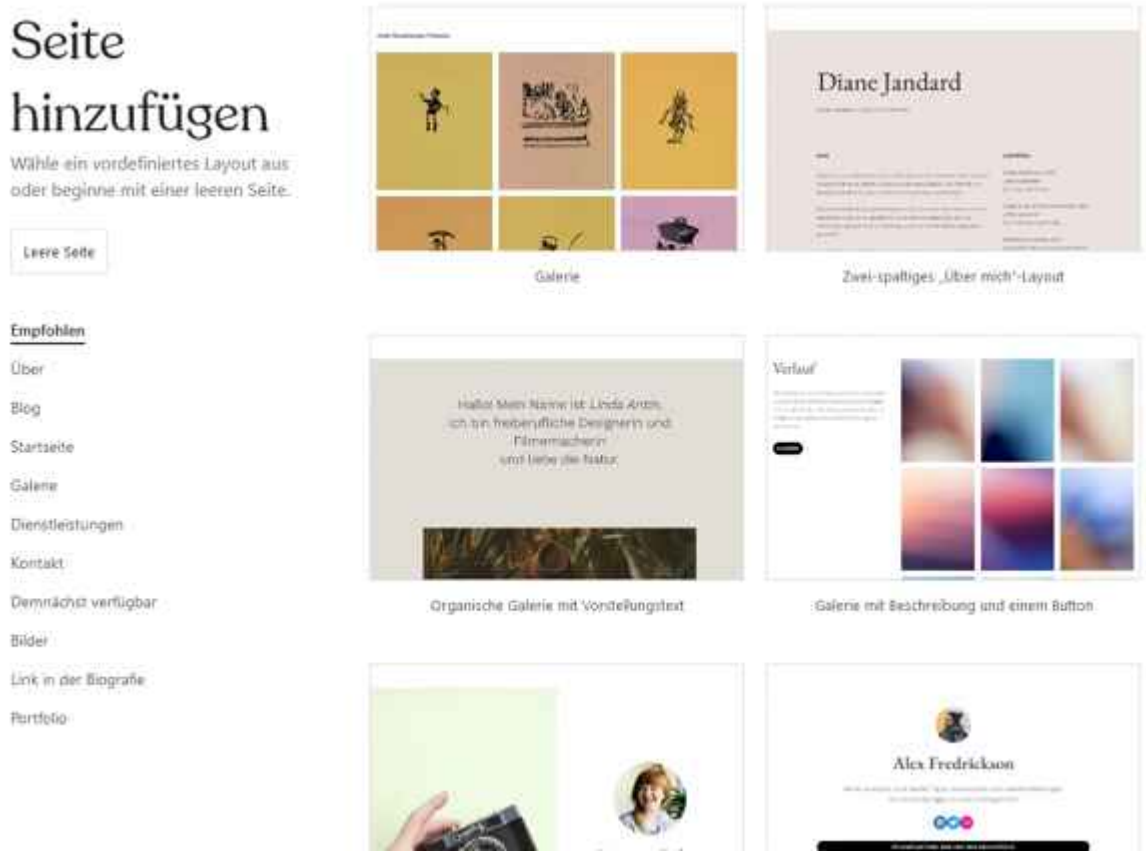
Sie sollten zudem beachten, ob ein ausgewähltes Theme sogenannte Pagebuilder von Fremdanbietern einbindet. Sie ergänzen den Editor mit vielen einfach nutzbaren Bauelementen wie Galerien, Buttons und Textbereichen, die Sie per Drag & Drop in die Seite ziehen können. Pagebuilder sind mächtige Werkzeuge, die es Website-Betreibern einfach machen, schnell ein gutes Layout zusammenzuklicken. Einige Pagebuilder allerdings erzeugen unnötigen Code und machen die Webseiten fett und langsam.

Pagebuilder standen Pate für den Gutenberg-Editor, den WordPress mittlerweile nutzt, und der für viele Anwendungszwecke genügt. Daher stellt sich seit Erscheinen von Gutenberg die Frage nach dem Sinn und Zweck von Pagebuildern noch mehr als zuvor. Diese Übersicht stellt dennoch einige Themes vor, die auf Pagebuilder setzen – weil diese Themes sehr beliebt sind und weil „Pagebuilder“ nicht automatisch schlechte Performance bedeutet. Manche Pagebuilder arbeiten auch mit Gutenberg zusammen.

Die Erfahrung zeigt allerdings auch, dass es häufiger Ärger

bei Updates und Theme-Wechseln von Websites gibt, die Themes mit Pagebuildern nutzen. Wenn es sich machen lässt, sollten Sie beim Aufsetzen einer neuen Site daher auf solche Themes und Pagebuilder außer Gutenberg verzichten. Das gilt insbesondere, weil WordPress vor einem grundlegenden Wechsel der Themes-Architektur steht (siehe Absatz „Minimalistisch und elegant“), bei dem sich noch zeigen muss, wie die Entwickler von Pagebuildern damit umgehen wollen.

Wenn Sie Wert auf größtmögliche Flexibilität legen, sollten Sie darauf achten, dass das Theme sogenannte Hooks unterstützt. WordPress baut eine Seite aus diversen Datenbankabfragen zusammen. Dabei arbeitet der WordPress-Kern mit Plug-ins und dem Theme zusammen, um Seitenelemente wie Texte und Bilder zu sammeln und die Seite zu rendern. Mit Hooks können Entwickler ihren Code an bestimmten Punkten in diesen Erstellungsprozess einklinken und ausführen. Manche Themes ermöglichen es, auf Hooks durchzugreifen, was zusätzliche Layout-Möglichkeiten bietet. So können Sie zum Beispiel sehr einfach einen zusätzlichen Text oder ein zusätzliches Banner im Kopf Ihrer Site einfügen.



Mit dem Standard-Theme kann man neue Seiten von Vorlagen ableiten oder mit einer leeren Seite beginnen – für viele Zwecke genügt das schon.

Für umme

Bei Gratis-Themes geben die Entwickler in der Regel keinen Support. Nutzer helfen sich bei Schwierigkeiten gegenseitig im Forum, das es im WordPress-Themes-Verzeichnis für jedes Theme gibt. Den Link darauf finden Sie in der Sidebar der Themes-Seite. WordPress enthält von Haus aus mehrere Themes, die von den Entwicklern des CMS selbst stammen. Im Moment sind das **Twenty Nineteen**, **Twenty Twenty** sowie das aktuelle Theme **Twenty Twenty-One**. Alle Standard-Themes sind kostenlos. Grundsätzlich eignen sie sich insbesondere für Einsteiger hervorragend, da sie nicht mit Optionen und Features überhäuft sind.

Twenty Twenty-One, das aktuelle Standard-Theme, ist ideal abgestimmt auf den Gutenberg-Editor. Es versteht sich als leere Leinwand, auf der die Nutzer mithilfe der Gutenberg-Blöcke ihre eigenen Ideen und Vorstellung verwirklichen (wer

das nicht mag, findet aber auch ein paar Layoutvorlagen). Das Theme eignet sich somit für alle, die gerne mit den WordPress-eigenen Tools eine komplette Website entwerfen möchten. Da Sie mit dem Theme bei Null anfangen, stehen Ihnen damit alle Möglichkeiten offen – nicht nur Portfolio- und Business-Website sowie private Blogs, für die das Theme im Verzeichnis angepriesen wird.

GeneratePress eignet sich für viele verschiedene Einsatzmöglichkeiten, auch mit dem E-Commerce-Plug-in WooCommerce ist es kompatibel (siehe S. 73). Es ist daher sehr beliebt. Die Entwickler legen viel Wert auf gute Performance, Stabilität und Benutzerfreundlichkeit. Schon in der Basisversion bietet das Theme mit seinem responsiven Design, den neun Widget-Bereichen, fünf Navigationspositionen und fünf Seitenleisten-Layouts unzählige Möglichkeiten, um eine Website zu gestalten.

Die kostenpflichtige Premium-Version gewährt noch einmal deutlich mehr Design- und Gestaltungsmöglichkeiten. GeneratePress nutzt den WordPress-Customizer, mit dem man Layoutoptionen für das Theme bequem per Dialog einstellt, für besonders viele Optionen. Es lassen sich also besonders viele Einstellungen per Customizer setzen, für die man bei anderen Themes Hand an den Code legen müsste oder Plug-ins benötigt. Dazu gehören erweiterte Einstellungen für Farben, Schriften, Menüs, Header, Abstände und vieles mehr. Entwickler können auf eine Bibliothek vorgefertigter Layouts zugreifen, um ihr Design zu entwerfen. Zudem können Entwickler in der Premium-Version Hooks ansprechen.

Astra ist wie GeneratePress eines der beliebtesten Themes für WordPress. Das liegt daran, dass es sehr anpassbar und flexibel ist. Astra bietet zudem über 180 Designvorlagen, die allerdings teilweise mit – verschiedenen – Pagebuildern realisiert wurden. Wer ein kostenloses und schnelles Theme für einen WooCommerce-Shop sucht, der ist mit Astra sicherlich gut bedient. Das Theme ist zwar nicht nur auf Websites

ausgerichtet, die das Shop-Plug-in verwenden, findet aber in der WooCommerce-Community großen Anklang. Die kostenpflichtige Version bietet noch viele zusätzliche Möglichkeiten, darunter Hooks, um die Website an externe Datenquellen anzubinden

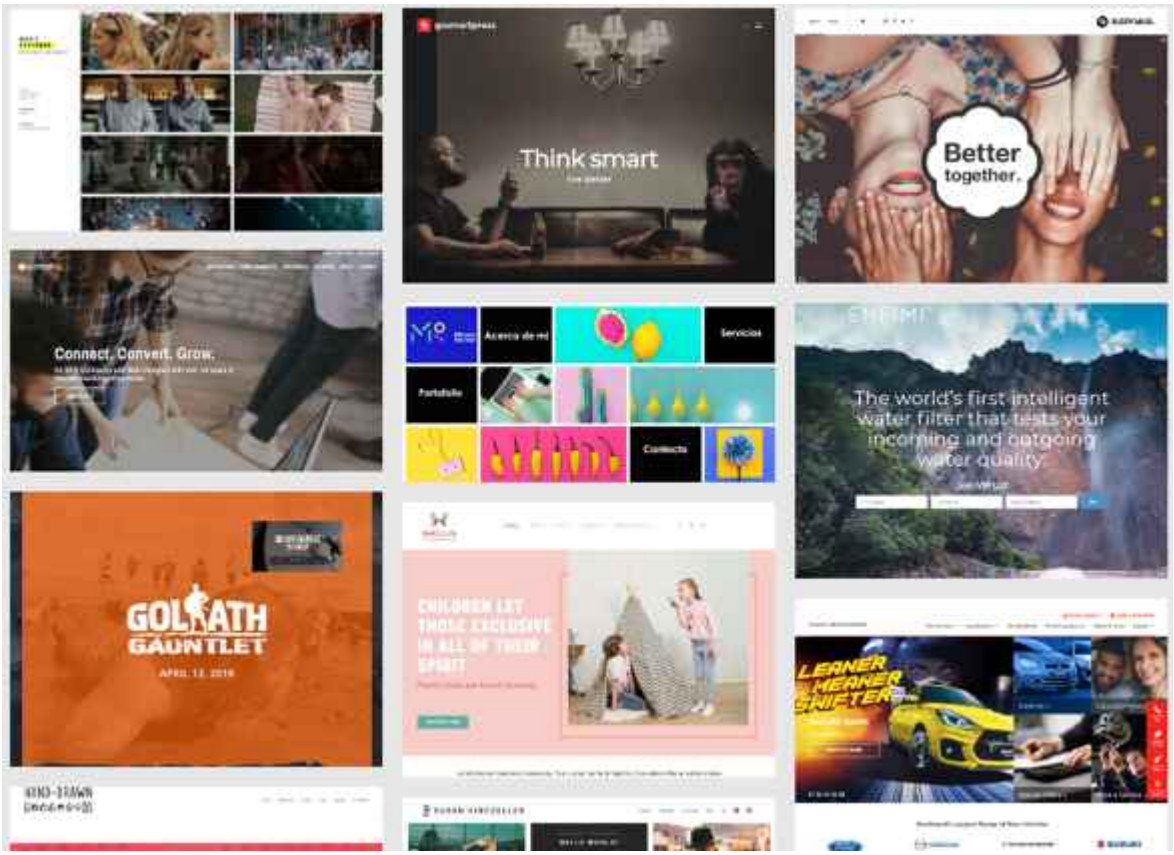
Premium-Themes

Die unschlagbaren Vorteile vieler Premium-Themes sind der Support und die Update-Frequenz, die oft deutlich höher ist als bei kostenlosen Themes. Auch bieten Premium-Themes mitunter Besonderheiten – etwa eine integrierte Shop-Funktion oder eine über einfache Links hinausgehende Social-Media-Vernetzung –, die man sonst erst umständlich nachrüsten muss. Viele Premium-Themes lassen sich außerdem für den Einsatz in verschiedenen Anwendungsbereichen anpassen. Durch die Fülle an Features und Möglichkeiten wirken Premium-Themes allerdings schnell sehr überladen und für unbedarfte Nutzer unübersichtlich.

Divi-Theme ist ein Allrounder für alle Fälle. Das Theme ist mit einem eigenen Pagebuilder ausgestattet. Mit Divi-Theme können Sie also eine Website von Grund auf gestalten. Kaum ein Theme liefert so viele verschiedene vorgefertigte Elemente mit. Zudem besticht Divi-Theme auch durch über 110 vorgefertigte Websites und etliche Layout-Elemente, etwa für Bilder-Slider und Formulare, die als Vorlage für eine eigene Website dienen können. Genau diese Vielzahl an Möglichkeiten ist es aber auch, die Einsteiger und Anfänger verunsichern kann. Nutzer, die keine Erfahrung im Webdesign haben, sollten zu einem der kostenlosen und einfacheren Themes greifen. Mit seiner umfangreichen Dokumentation und sehr großen Community sowie dem guten Support gehört Divi-Theme aber zu Recht zu den beliebtesten WordPress-Themes.

Beim Premium-Theme **Enfold** wählen Sie als Ausgangspunkt für ein eigenes Design eine aus mehr als 35 Website-Vorlagen, etwa für Firmen- oder Restaurant-Homepages, Blogs oder Onepager. Das Theme bietet vor allem für die Gestaltung von Portfolio-

Websites umfangreiche Möglichkeiten. Durch den eigenen Pagebuilder bietet Enfold eine Vielzahl von eigenen Elementen zur Gestaltung der Website. Die Community ist sehr engagiert und der Support außerordentlich gut – und deutschsprachig, weil die Entwickler Österreicher sind.



Die Themes-Entwickler unterhalten Galerien, in denen man sich einen Eindruck von den Möglichkeiten ihrer Werke – hier: Enfold – machen kann.

Minimalistisch und elegant

Das Werkstatt-Theme von Elmastudio eignet sich gut zur Präsentation von Portfolios.
Wer es gerne aufgeräumt und minimalistisch mag, der sollte sich die Themes von **Elmastudio** ansehen. Sie sind allesamt klar und elegant im Design. Künstler oder Fotografen sollten hier ein Theme finden, mit dem sie Ihr Portfolio gut in Szene setzen können. Die 18 Themes kosten einzeln 19 Euro und im Paket 39 Euro inklusive einem Jahr Updates.

Hervorzuheben ist das Theme **Aino**, das bereits als sogenanntes Full-Site-Editing-Theme zur Verfügung steht. Full Site Editing bedeutet, dass WordPress-Seiten zukünftig ausschließlich aus Blöcken bestehen soll, wie man sie im Gutenberg-Editor entwirft (siehe S. 64).

WordPress-Nutzer werden also auf alle Bereiche ihrer Website direkt im Editor zugreifen und diese bearbeiten können. Full Site Editing ist noch nicht vollständig in WordPress implementiert. Es ist daher nicht empfehlenswert, das Theme bereits produktiv einzusetzen. Man kann sich aber schon mal einen Eindruck davon verschaffen, wie sich Full Site Editing

anfühlt. Es soll voraussichtlich mit WordPress 5.9, welches im Dezember 2021 veröffentlicht wird, vollständig implementiert sein. Durch das Full Site Editing wird sich der Anbieter-Markt der Themes sicherlich neu sortieren, sodass für 2022 spannende Entwicklungen zu erwarten sind.

Sie haben unter den hier vorgestellten kein passendes Theme gefunden? Kein Problem, schließlich gibt es noch Tausende mehr im Verzeichnis von WordPress. (*jo@ct.de*)

Themes und -Verzeichnisse: ct.de/y8ea

WordPress – Erste Schritte

Websites bauen

Um ein Blog oder eine Website zu starten, brauchen Sie mit WordPress nur ein paar Minuten. Anders als bei Facebook, Instagram und anderen Plattformen legen Sie die Regeln fest

und gestalten den Auftritt nach eigenem Gusto.

Erste Schritte mit WordPress

Um ein Blog oder eine Website zu starten, brauchen Sie mit WordPress nur ein paar Minuten. Anders als bei Facebook, Instagram und anderen Plattformen legen Sie die Regeln fest und gestalten den Auftritt nach eigenem Gusto.

Von Daniel Berger

Den einfachsten Einstieg in die WordPress-Welt bieten spezielle Hoster, allen voran das Mutterunternehmen Automattic, das Sie unter wordpress.com finden. (Im Gegensatz zum WordPress-System selbst, das Sie unter wordpress.org finden.) Sie brauchen keinen eigenen Webspace oder gar Server – einfach anmelden und schon kanns losgehen. Um Updates und Wartung müssen Sie sich nicht kümmern, allerdings sind die Funktionen eingeschränkt – insbesondere in der kostenlosen Variante, bei der Sie außerdem mit Werbeanzeigen in Ihrem Blog leben müssen.

Der Dienst eignet sich aber bestens, um WordPress schnell mal auszuprobieren und einen Blick in die Verwaltung zu werfen, das sogenannte Backend. Die dort angelegten Inhalte lassen sich jederzeit exportieren und in eine andere WordPress-Instanz importieren, zum Beispiel in eine selbst gehostete. Viele andere Webhoster bieten WordPress als sogenannte 1-Klick-Installation an, die das Content-Management-System (CMS) inklusive der benötigten Datenbank automatisch einrichtet.

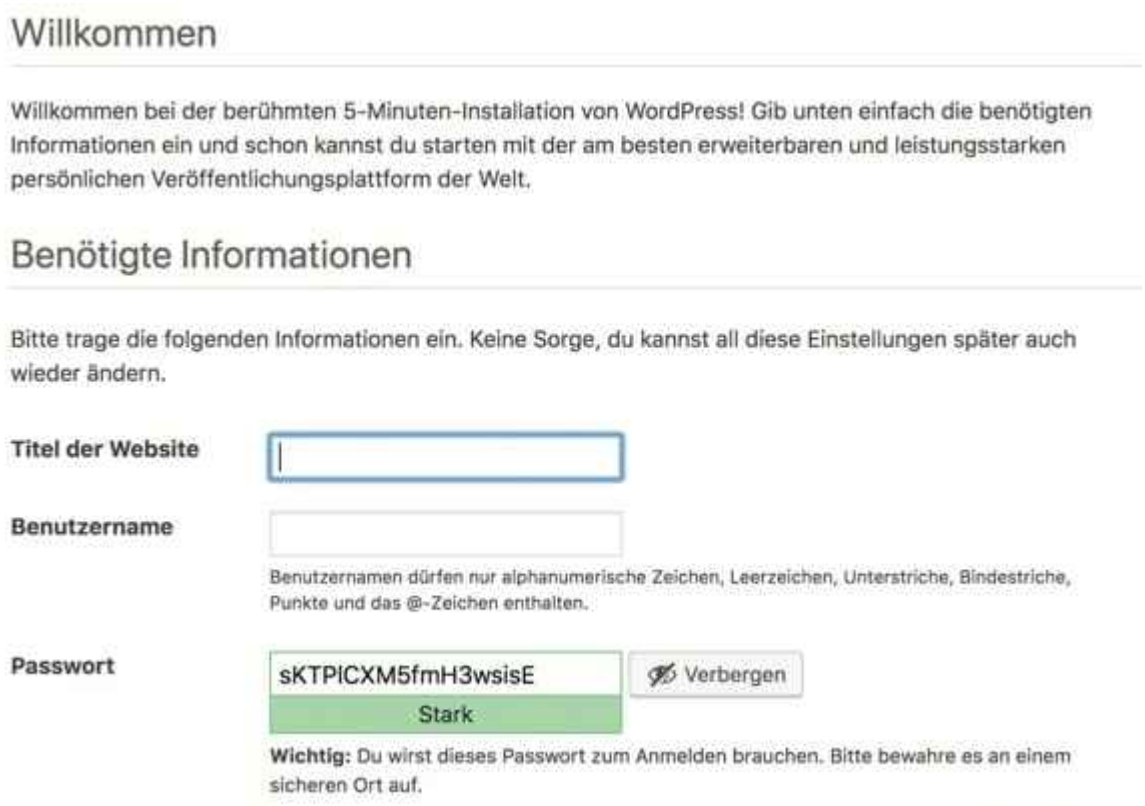
Die größte Freiheit bietet eine selbst vorgenommene WordPress-Installation. Geeigneten Webspace gibt es bereits ab 3 Euro im Monat. Es geht zwar auch billiger, aber dann ist die Performance eventuell nicht top und die Website lahmt. Wichtig ist, dass das Hosting-Paket mindestens PHP 7.4 und MySQL oder MariaDB unterstützt, was aber inzwischen zur

Standardausstattung gehört.

Die ins Deutsche übersetzte Version des CMS laden Sie auf de.wordpress.org mit einem Klick auf „Hol dir WordPress“ herunter (alle Links siehe ct.de/yj1e). WordPress selbst wirbt mit der „berühmten 5-Minuten-Installation“. Die ist kein leeres Versprechen, denn auch die manuelle Einrichtung kostet tatsächlich nicht viel Zeit. Entpacken Sie zunächst die heruntergeladene Zip-Datei und laden Sie die Ordner und Dateien auf Ihren Webspace.

Während des Hochladens können Sie schon mal über die Web-Admin-Oberfläche Ihres Hosters eine MySQL- oder MariaDB-Datenbank anlegen. In der speichert WordPress alle Beiträge, Seiten, Kommentare, Einstellungen und Metadaten. Das Vorgehen ist von Anbieter zu Anbieter unterschiedlich. Meistens finden Sie dort aber einen Menüpunkt „Datenbanken“, wo Sie weitgehend automatisiert eine neue Datenbank anlegen können. In der Regel bestimmen Sie das Passwort selbst. Wählen Sie schon bei der Ersteinrichtung ein sicheres Passwort, das mindestens 12 Zeichen lang und in keinem Wörterbuch zu finden ist.

Halten Sie Datenbank-Namen, -Nutzernamen und -Passwort griffbereit, sie werden bei der WordPress-Einrichtung abgefragt. Nach erfolgreichem Hochladen starten Sie das Installationsskript, indem Sie die Datei wp-admin/install.php im Browser aufrufen. Die genaue URL hängt von Ihrer Domain ab und davon, in welchen (Unter-)Ordner Sie die Dateien geladen haben. Folgen Sie den wenigen Anweisungen des Skripts im Browser. Kommt es zu Problemen, sind meistens die Schreibrechte nicht korrekt eingestellt. Die überprüfen Sie ebenfalls über die Verwaltungsoberfläche des Hosters. Ansonsten gibt die Onlinehilfe von WordPress gute Ratschläge (siehe ct.de/yj1e).



Nur drei Felder ausfüllen, fünf Minuten später ist die Installation von WordPress tatsächlich erledigt.

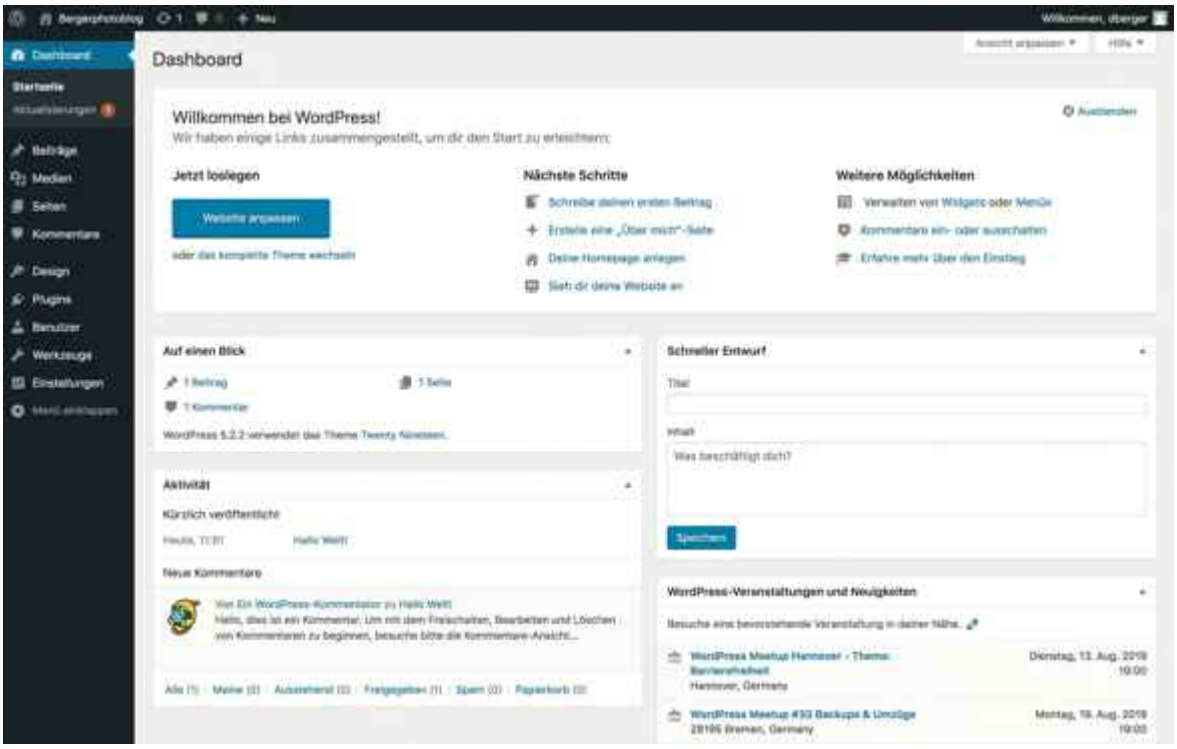
Das Dashboard erkunden

Nach der Installation öffnen Sie zunächst den Administrationsbereich – das Backend – von WordPress, indem Sie im Browser …/wp-admin aufrufen. Die nötigen Login-Daten haben Sie bei der Installation festgelegt. Im Backend begrüßt Sie das Dashboard des CMS, das Ihnen einen schnellen Überblick verschafft. Mit dem Knopf „Ansicht anpassen“ oben rechts steuern Sie, welche Informationen das Dashboard anzeigen soll. Haben Sie Interesse am Austausch mit anderen Nutzern, finden Sie in der Box „WordPress-Veranstaltungen und Neuigkeiten“ Hinweise zu Meetups der WordPress-Community und Events in der Gegend.

Sollten Sie ganz plötzlich die beste Idee der Welt haben, können Sie die als „Schnellen Entwurf“ blitzschnell direkt ins Dashboard hacken. Ein Klick auf „Speichern“ erzeugt einen Blogbeitrag, der aber nicht sofort online geht – perfekt für Notizen und Entwürfe. Doch Vorsicht: Anders als im Haupt-

Editor speichert WordPress im Dashboard nicht automatisch zwischen.

Die „Schneller Entwurf“-Box zeigt auch die letzten Entwürfe an. Der Bereich „Aktivitäten“ informiert über neue Kommentare, die Sie direkt beantworten, bearbeiten, zurückweisen oder löschen können. Ein Klick auf „Papierkorb“ schickt die Kommentare genau dorthin. Die „Hilfe“ gibt Unterstützung beim Navigieren durchs CMS. Wenn Sie später Plug-ins installieren, tauchen eventuell weitere Boxen im Dashboard auf, die beispielsweise Besucherzahlen ausweisen.



Das Dashboard ist die Schaltzentrale jeder WordPress-Seite.

Einstellungen vornehmen

Ein erster Ausflug führt Sie in die Einstellungen von WordPress, wo Sie grundlegende Informationen zu Ihrem Internetauftritt festlegen. Dazu gehören etwa der „Website-Titel“ und ihr „Untertitel“ oder Slogan. Das aktive Theme bestimmt, wo und wie Titel und Slogan auf der Website zu sehen sind und ganz generell, wie Ihre Website aussieht. Es gibt Themes in Hülle und Fülle – für jeden Zweck steht das passende Kleid bereit. Bereits installiert sind bei WordPress die

Standard-Themes „Twenty Twenty-One“, „Twenty Twenty“ und „Twenty Nineteen“. Ungefähr jedes Jahr kommt ein neues hinzu, entwickelt werden Sie von wordpress.org selbst. Der Artikel auf Seite 68 stellt eine Reihe schicker Designs vor.

Eine weitere wichtige Einstellung betrifft die Links, die WordPress zu den Beiträgen und Seiten erzeugt, die sogenannten „Permalinks“. Deren URL-Struktur können Sie frei bestimmen. Sinnvoll ist beispielsweise eine Struktur, die Kategorie und Titel einer Seite berücksichtigt, was zu URLs wie …/rezepte/salami-pizza führt. Zum einen erhöht das die Nutzerfreundlichkeit. Zum anderen sind wichtige Schlagworte enthalten, die wiederum Google helfen, den Inhalt richtig einzuordnen (Rezept/Pizza). Eine URL wie …/?p=235 ist zwar auch möglich, aber zu kryptisch, als dass sie irgendwem weiterhelfen würde. Die Struktur der Permalinks lässt sich jederzeit ändern, aber nachträgliche Änderungen können negative Auswirkungen aufs Google-Ranking haben.

Geschäftlich oder privat?

Möchten Sie ein rein privates Blog führen, das nicht bei Google auftauchen soll, setzen Sie in den Einstellungen unter „Lesen“ ein Häkchen bei „Suchmaschinen daran hindern, diese Website zu indexieren“. Aber Vorsicht: Bekannte Anbieter wie Google oder Bing halten sich an diese Vorgabe, aber manch andere Suchmaschine setzt sich darüber einfach hinweg. Außerdem bleiben Ihre Einträge auch mit dieser Einstellung öffentlich zugänglich. (Das ändern Sie, wenn Sie für einen Beitrag ein Passwort festlegen oder seine Sichtbarkeit auf „privat“ stellen.)

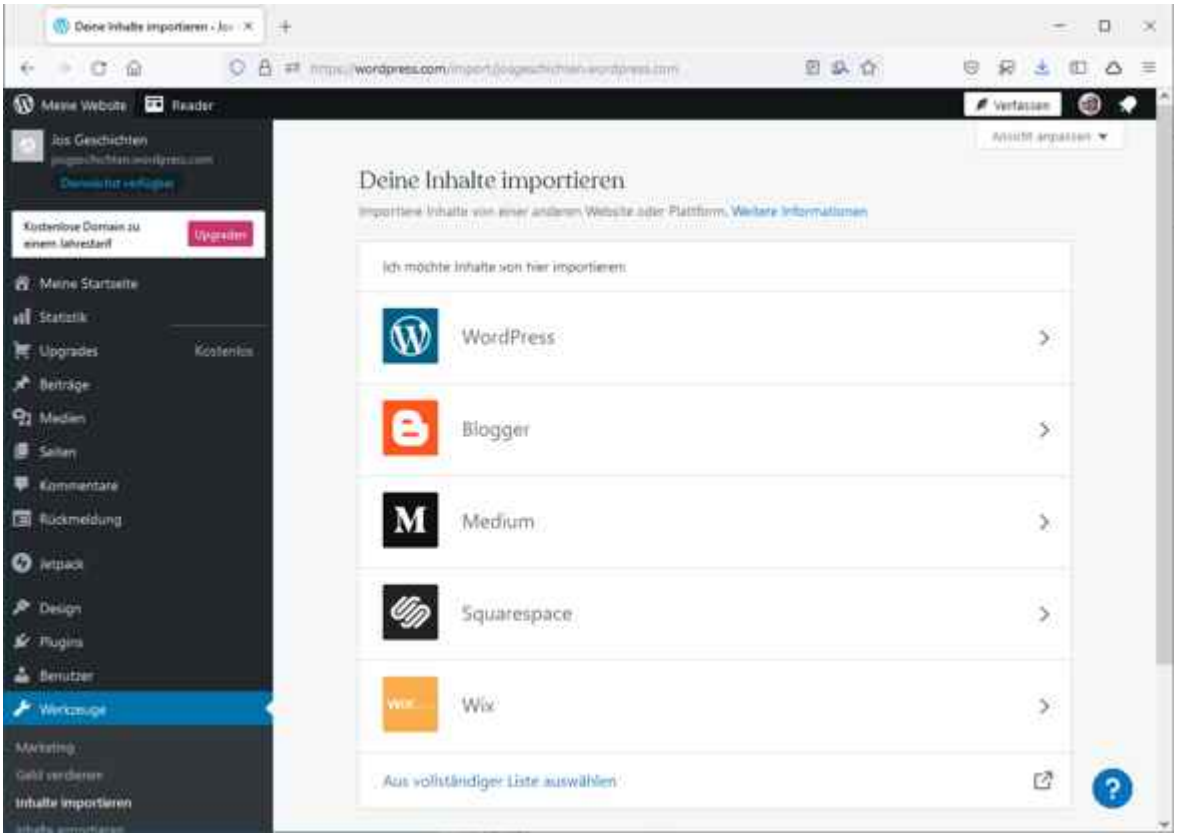
Sie haben keine Lust auf doofe Kommentare? Unter „Diskussion“ schalten Sie die Funktion einfach ab („Besuchern erlauben, neue Beiträge zu kommentieren“). Alternativ gibt es die Option, nur Nutzer kommentieren zu lassen, die sich registriert haben, und sich vom CMS per Mail informieren zu lassen, wenn ein neuer Kommentar eintrifft oder auf

Freischaltung wartet. Für letzteres müssen Sie in den Einstellungen festlegt haben, dass Kommentare manuell freigeschaltet werden müssen, ehe sie öffentlich zu sehen sind.

Nicht alle Einstellungen finden sich in dem so bezeichneten Menüpunkt. Wenn Sie bereits ein Blog betreiben oder ein altes Exemplar sichern möchten, können Sie dessen Inhalte einfach importieren – unter „Werkzeuge“. WordPress unterstützt von Haus aus Blogger.com von Google, Tumblr, LiveJournal, Movable Type und TypePad. Sie können außerdem Beiträge über einen RSS-Feed importieren. Ergänzend nimmt das CMS Links im OPML-Format entgegen. Weitere Importer für Spezialfälle gibt es als Erweiterungen in WordPress’ Plug-in-Verzeichnis.

WordPress bietet also viele Einstellungsmöglichkeiten, die im Admin-Bereich jedoch an verschiedenen Stellen verteilt sind. Wenn Sie mehrere Optionen auf einen Schlag anpassen oder eine bestimmte Option schnell finden wollen, werfen Sie einen Blick auf die URL …/wp-admin/options.php. Dort führt das CMS alle verfügbaren Einstellungen in einer alphabetisch sortierten Liste auf.

Besonders nutzerfreundlich ist die Ansicht allerdings nicht. Die englischsprachigen Optionen dort sind unkommentiert und entsprechen nicht mal Bezeichnungen der englischen Bedienoberfläche. Man muss sich also zusammenreimen, dass mit „blogname“ und „blogdescription“ der Website-Titel und -Untertitel gemeint sind. Änderungen werden in den Textfeldern vorgenommen. Auf diese Weise editieren Sie etwa die Admin-Mailadresse, den Blognamen oder die Reihenfolge der Kommentare in einem Rutsch. Vergessen Sie nicht, am Ende der langen Seite auf „Speichern“ zu klicken.



Umzugshilfe: WordPress kann Beiträge aus anderen Plattformen importieren.

Der Gutenberg-Editor

WordPress verwaltet die Inhalte als „Beiträge“ (Posts) und als „Seiten“ (Pages). Beiträge sind für Blog-Posts, Nachrichten und Neuigkeiten gedacht. Viele Themes listen sie in umgekehrt chronologischer Reihenfolge auf der Startseite auf – so sind klassische Blogs aufgebaut. Um einen Beitrag hervorzuheben, setzen Sie ein Häkchen bei „Beitrag auf der Startseite halten“. Der Beitrag bleibt nun auch dann ganz oben, wenn Sie neuere Inhalte veröffentlichen. Wie genau der festgepinnte Post den Seitenbesuchern dargestellt wird, hängt vom verwendeten Theme ab.

Das Herzstück von WordPress ist der Editor für Beiträge und Seiten. Der verursachte Ende 2018 hitzige Diskussionen, denn mit dem Release von WordPress 5.0 ersetzte der neue Gutenberg-Editor den alten TinyMCE-Editor. Seit Gutenberg müssen die Nutzer in Blöcken denken: Ein Textabsatz ist ein Block, ein Bild ist ein Block, eine Überschrift ist ein Block – kurz:

Jedes Element ist ein Block. Diese Inhaltsblöcke lassen sich einfach verschieben, umsortieren und individuell konfigurieren. Gutenberg macht den Aufbau von Webseiten, die kein lineares Textdokument sind, sehr viel leichter, als es zuvor mit TinyMCE möglich war.

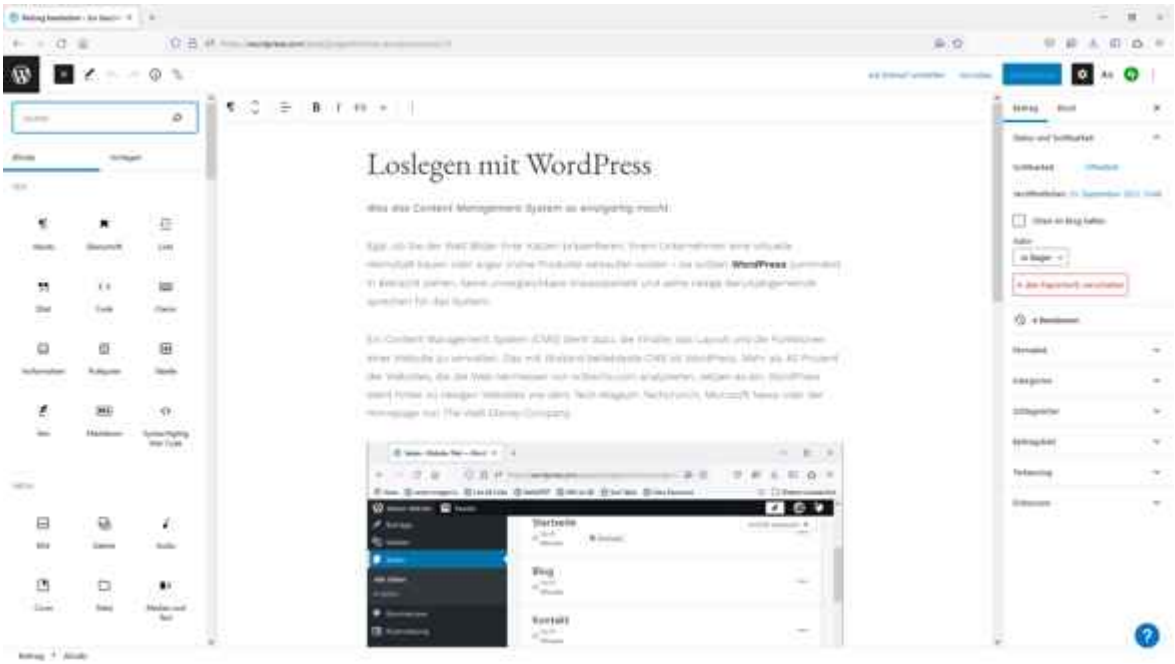
Probieren Sie ihn aus und legen Sie unter „Beiträge/Erstellen“ einen neuen Post an. Über das Plus-Symbol links oben oder die Plus-Symbole im Dokument fügen Sie neue Blöcke hinzu. Um ein Foto einzufügen, wählen Sie den allgemeinen Block „Bild“ aus. Ganze Alben lassen sich per „Galerie“ in einen Beitrag einbetten. Für Experten gibt es zum Beispiel das kleine HTML-Icon, um eigenen Code einzufügen.

Unter dem Reiter „Beitrag“ (in der rechten Seitenleiste; in nicht ganz aktuellen WordPress-Versionen heißt der Reiter „Dokument“) legen Sie den individuellen Status und die Sichtbarkeit des Beitrags fest. Sie können auch ein Passwort vergeben: Nur wer es kennt, kann den Text lesen. Wenn Sie die Sichtbarkeit auf „Privat“ stellen, sehen nur Admins und registrierte Redakteure den Beitrag. In den Beitrag-Einstellungen bestimmen Sie außerdem Kategorien, Schlagworte (Tags) und das Beitragsbild. Dort können Sie auch die Kommentar-Funktion für einzelne Beiträge deaktivieren.

Der Reiter „Block“ bezieht sich auf den jeweiligen aktiven Block, den Sie links im Editor gerade bearbeiten. Die verfügbaren Einstellungen sind vom Block-Typ abhängig. Bei einem Textblock können Sie etwa eine CSS-Klasse unter „Erweitert“ festlegen, die dem Block zugeordnet wird. Sinnvoll ist das zum Beispiel für einen Texteinstieg, der gesondert hervorgehoben werden soll.

Die Möglichkeiten sind vom aktivierten Theme abhängig, viele bieten für den Texteinstieg zum Beispiel eine CSS-Klasse „intro“ an. Hinzu kommen die Text- und Farbeinstellungen, die ebenfalls vom Theme abhängig sind. Probieren Sie ruhig alle Optionen aus – solange Sie nicht auf „Veröffentlichen“ (rechts

oben) klicken, kann niemand sehen, was Sie fabrizieren.



Im Gutenberg-Editor finden Sie links die Content-Blöcke und rechts allgemeine Optionen für den Beitrag.

Statische Seiten

Im Unterschied zu den Beiträgen sind „Seiten“ für statische Inhalte gedacht, die sich nicht oft ändern, also etwa für eine Kontakt- oder eine Über-mich-Seite. Weil Seiten keine Beiträge sind, tauchen sie nicht automatisch in den Übersichten auf. Betreiben Sie mit WordPress kein Blog, sondern eher eine herkömmliche Website, können Sie alle Unterseiten Ihrer Präsenz als statische Seiten anlegen. Auf diese Weise ist etwa eine einfache Firmenpräsenz fix eingerichtet. Nach der Seiten-Struktur richtet sich auch die URL-Struktur: Ist die Seite „Team“ eine Unterseite von „Firma“, lautet ihre URL also: …/firma/team. Anders als die Beiträge verwenden Seiten keine Schlagwörter und keine Kategorien.

In der Seitenleiste des Editors weisen Sie unter „Seite/Seiten-Attribute“ einer Seite ein bestimmtes „Template“ (Vorlage) zu, sofern das Theme Templates vorsieht. Damit bringen Sie auf einfache Art etwas Abwechslung in das Aussehen Ihrer Website und trotzdem ist optisch noch alles aus einem

Guss. Templates können zum Beispiel die Seitenleiste eines Themes ausblenden und den Text über die gesamte Breite laufen lassen. Bei „übergeordnete Seite“ legen Sie die Elternseite fest.

Die Option „Reihenfolge“, ebenfalls bei den Seiten-Attributen, steuert ebendiese. Die Werte sind beliebig: Wenn Sie wollen, ordnen Sie einer Seite eine „99“ zu und der anderen eine „999“. Unter „Seiten/Alle Seiten“ listet WordPress die angelegten Seiten in der vom Nutzer festgelegten Reihenfolge auf. Ist keine Reihenfolge und keine „übergeordnete Seite“ festgelegt, sortiert WordPress die Einträge von A bis Z.

Zu den ersten Seiten, die Sie anlegen sollten, zählen ein Impressum und eine Datenschutzerklärung – sonst drohen Abmahnungen, insbesondere, wenn Sie einen Onlineshop betreiben oder anderweitige kommerzielle Interessen verfolgen. Hilfreiche Hinweise, was dabei zu beachten ist, finden Sie zum Beispiel bei datenschutz.org (ct.de/yj1e). Im Reiter „Seite“ finden Sie auch die Versionskontrolle. Sie stellt sicher, dass ältere Textvarianten nicht verloren gehen. Jeder kann nachvollziehen, wer was wann geändert hat. Sie öffnen sie mit einem Klick auf den Link mit dem Uhren-Symbol.

Medien und Themes

Hinter dem Menüpunkt „Medien“ im WordPress-Backend verbirgt sich die Mediathek von WordPress. Sie versammelt alle hochgeladenen Bilder, Videos, Audiodateien und Dokumente an einem zentralen Ort. Über die beiden Drop-down-Menüs in der Toolbar wählen Sie Inhalte gezielt nach Medientyp oder nach Upload-Monat aus. Auf der rechten Seite hilft ein Suchfeld beim gezielten Aufspüren von Inhalten.

In der Mediathek können Sie ausmisten oder neue Materialien hochladen, die Sie später in Blog-Einträgen und Seiten verwenden möchten. An dieser Stelle versehen Sie die Inhalte außerdem mit Metadaten – sie sind für die Suchfunktion und vor

allem für Google relevant. Dessen Bildersuche ist für viele Blogs ein wichtiger Traffic-Lieferant: Ein Reiseblog etwa kann allein durch gute Fotos viele Nutzer anlocken. Versuchen Sie zudem, bei den Bildunterschriften wichtige Suchbegriffe einzubauen, wenn Sie Bilder in ihre Seiten und Beiträge einbauen.

Um ein Bild mit Metadaten und weiteren Informationen zu versehen, klicken Sie es in der Übersicht an. Hier geben Sie zusätzlich einen „alternativen Text“ (ALT-Tag) ein, der das Bild beschreibt. Die Angabe ist optional, hilft aber Menschen mit Sehbehinderung, die einen Screenreader verwenden. Der Button unter dem Bild führt zu einer einfachen Bildbearbeitung, mit der Sie etwa Fotos beschneiden, drehen und spiegeln können. Photoshop ersetzt sie zwar nicht, aber kleine Korrekturen sind schnell vorgenommen.

Benutzer verwalten

Zusammen ist man weniger allein, das gilt auch beim Bloggen. Sie können weitere Mitstreiter, Autoren und Entwickler unter dem Menüpunkt „Benutzer“ anlegen und ihnen unterschiedliche Zugriffsrechte einräumen. Achten Sie darauf, wem Sie welche Rollen zuweisen: Wenn Sie einen weiteren Benutzer als „Admin“ hinzufügen, bekommt derjenige volle Eigentümerrechte und kann das gesamte Blog löschen. WordPress selbst empfiehlt daher nur einen Admin pro Blog.

Wählen Sie für Mitstreiter lieber die Rolle „Redakteur“ aus. Ein solcher kann Beiträge und Seiten ansehen, bearbeiten, veröffentlichen und löschen. Außerdem dürfen sich Redakteure um die Kommentare kümmern sowie Kategorien und Schlagworte verwalten. Ein „Autor“ darf nur seine eigenen Inhalte bearbeiten und veröffentlichen. Ein „Mitarbeiter“ darf Beiträge schreiben, sie aber nicht selbst freigeben. Über „Benutzer/Neu hinzufügen“ legen Sie neue Benutzerkonten an und vergeben die gewünschten Rollen. Die eigenen persönlichen Optionen finden Sie (und alle anderen Nutzer) unter

„Benutzer/Dein Profil“.

Besucher der Website können sich auch selbst als Nutzer registrieren, wenn Sie das in den allgemeinen Einstellungen über „Jeder kann sich registrieren“ erlauben. Das ist zum Beispiel nützlich, wenn Sie nur von registrierten Benutzern Kommentare zulassen wollen. In den Einstellungen legen Sie auch die Rolle für solche neuen Benutzer fest, in der Regel sollte das „Abonnent“ sein.

Bei Blogs, die auf wordpress.com gehostet werden oder das Jetpack-Plug-in nutzen (siehe S. 72), können sich die Leser zudem als „Follower“ anmelden. Dann bekommen sie per E-Mail Bescheid, wenn es neue Inhalte gibt. Wenn Sie ein Häkchen bei „Benutzer benachrichtigen“ setzen, erhält dieser eine Einladung.

Effizienter bloggen

Die Verwaltungsarbeit in WordPress kostet etwas Zeit – kann aber beschleunigt werden. In der Beiträge- und Seiten-Übersicht lassen sich zum Beispiel die Inhalte massenweise editieren. Um etwa die Kategorien von gleich mehreren Beiträgen zu bearbeiten, markieren Sie zunächst die entsprechenden Posts. Dann wählen Sie im Drop-down-Menü „Mehrfachaktionen“ den Punkt „Bearbeiten“ und klicken auf „Übernehmen“.

Es öffnet sich die „Mehrfachbearbeitung“, in der Sie Kategorien und Schlagworte ändern und hinzufügen können. Außerdem haben Sie die Möglichkeit, den Autor und den Status der Beiträge zu ändern sowie die Kommentarfunktion abzuschalten. Sind alle Änderungen vorgenommen, klicken Sie abschließend auf „Aktualisieren“. Die eingesparte Zeit steht nun fürs eigentliche Bloggen zur Verfügung.

Und auch das Schreiben und Formatieren lässt sich effizienter gestalten, denn der Gutenberg-Editor unterstützt diverse

Tastenkürzel. Strg+B fettet ein markiertes Wort, Strg+I setzt es kursiv, Strg+U unterstreicht es. Dann gibt es die aus Software bekannten Kürzel: Strg+S speichert den Beitrag, Strg+Z macht die letzte Änderung rückgängig (unter macOS gelten die entsprechenden Befehle mit Cmd statt Strg). Mit Strg+K verlinken Sie den ausgewählten Text.

Praktisch sind die speziellen „Block"-Tastaturkürzel: Umschalt+Strg+D dupliziert den im Editor ausgewählten Block, Alt+Strg+Y fügt einen neuen Block nach dem ausgewählten ein. Für eine Übersicht aller verfügbaren Tastaturkürzel im Editor drücken Sie Umschalt+Alt+H (macOS: Ctrl+Alt+H) – oder Sie klicken auf das Icon mit den drei Punkten ganz oben in der rechten Ecke und dann auf „Tastaturkürzel".

Es gibt auch Tastaturkürzel, um die Arbeit in der Kommentarverwaltung von WordPress zu erleichtern. Die Funktion müssen Sie aber zunächst in den Einstellungen unter „Benutzer/Dein Profil" einschalten, indem Sie bei „Tastaturkürzel" ein Häkchen setzen. Anschließend können Sie mit J die Kommentare durchlaufen. Der jeweils aktive Kommentar ist hellblau eingefärbt.

Mit K springen Sie zum vorherigen Kommentar zurück. Um einen irrtümlich als Spam markierten Beitrag doch freizuschalten, drücken Sie A (für approve). Ein Tastendruck auf D verschiebt ihn in den Papierkorb (delete), ein Druck auf S markiert ihn als Spam. Mit Q aktivieren Sie den Quick Edit und können fix Fehler in einem Kommentar verbessern.

Ein Druck auf R löst eine Antwort auf Kommentar aus (reply). Mit den Tastaturkürzeln lassen sich auch mehrere Kommentare auf einen Schlag verwalten: Markieren Sie die Einträge mit X und drücken Sie dann Umschalt+S, um alle als Spam zu markieren. Umschalt+A, Umschalt+D und so weiter funktionieren analog. So herrscht schnell wieder Ordnung.

Erfolgreich im Netz

Der Anfang mit WordPress ist superleicht, dann heißt es aber: nicht nachlassen und motiviert am Ball bleiben. Am besten schreiben Sie bereits ein paar Einträge oder Seiten, noch bevor Ihre Website online geht. Dann haben die ersten Besucher gleich etwas zu lesen und auch der Google-Crawler findet genügend Material bei der ersten Indexierung. Wer nach dem Start seine Site regelmäßig mit guten Texten füllt, wird früher oder später seine Leser finden.

Insbesondere beim Bloggen zählt die persönliche Note. Schreiben Sie über ein Thema, mit dem Sie sich gern beschäftigen. Dass Sie mit Leidenschaft dabei sind, merken dann auch die Leser und honorieren Ihre Mühen zum Beispiel mit Feedback. Leser lieben außerdem Mehrwert: Das können Tipps fürs Reisen sein oder ausführliche Erfahrungsberichte, Anleitungen oder persönliche Produktbesprechungen.

Wenn Sie nun aber das tausendste Gadget-Blog gründen, das über iPhones berichtet, sind Sie sofort von harter Konkurrenz umgeben. Es dürfte schwer werden, ein Alleinstellungsmerkmal herauszuarbeiten. Einfacher gelingt der Start in einer Nische, in der es weniger Konkurrenz gibt und die Zielgruppe spitzer definiert ist. Spezialisieren Sie sich also – denn egal, wie abseitig Ihr Thema dann auch sein mag, es wird irgendwann sein Publikum finden.

Auf langweilige Texte reagieren allerdings nur wenige Leser. Wer mehr Kommentare will, darf durchaus mal ein bisschen frecher formulieren. Für viele Poster ist Feedback der größte Motivator. Versuchen Sie also, auf die Kommentare einzugehen, am besten auf jeden einzelnen. Humor hilft, besonders wenn Trolle Sie ärgern; außerdem können Sie Kommentare auch in den Papierkorb verschieben, schließlich ist das Ihre Website und Sie entscheiden über die Inhalte. Zudem sollten Sie Aufforderungen zu kriminellen Handlungen oder dubiose Links in den Kommentaren lieber entfernen.

Für den (schnellen) Erfolg kann etwas Eigenwerbung nicht schaden. Als Werbekanäle bestens geeignet sind ein ergänzender Instagram-Account sowie eine Seite bei Facebook. Auf beiden Plattformen verweisen Sie auf neue Blog-Einträge und tauschen sich mit Fans aus. Doch Vorsicht: So mancher Blogger ließ sich von Instagram verführen und veröffentlichte eines Tages nur noch dort. Das ist sehr schade, schließlich gehen viele Freiheiten verloren.

Updates nicht vergessen

Am Ball bleiben müssen Sie auch in puncto Sicherheit: Von Zeit zu Zeit kommen Sicherheitslücken in WordPress ans Licht, die aber meist schnell gestopft werden. Wichtig ist, dass Sie brav jedes Update einspielen und damit das CMS auf dem neuesten Stand halten. Die kleineren Sicherheitsaktualisierungen installiert WordPress bequem automatisch, zur Bestätigung erhalten Sie eine E-Mail.

Um größere Versionssprünge müssen Sie sich aber selbst kümmern. Plug-ins und Themes aktualisieren sich ebenfalls nicht von selbst. Die Updates für Erweiterungen sind genauso wichtig wie die fürs CMS, denn sie gehören zu den größten Einfallstoren für Schadcode. Viel Aufwand machen diese Updates glücklicherweise nicht, es sind nur wenige Klicks nötig. Unter dem Menüpunkt „Dashboard/Aktualisierungen“ können Sie schnell prüfen, ob die neuesten Versionen der Themes, Plug-ins, Übersetzungen und von WordPress selbst installiert sind.

Dies ist die gekürzte und überarbeitete Version eines Artikels, der zuerst in Mac & i extra Workshops erschien. (jo@ct.de)

Hilfeseiten: ct.de/yj1e