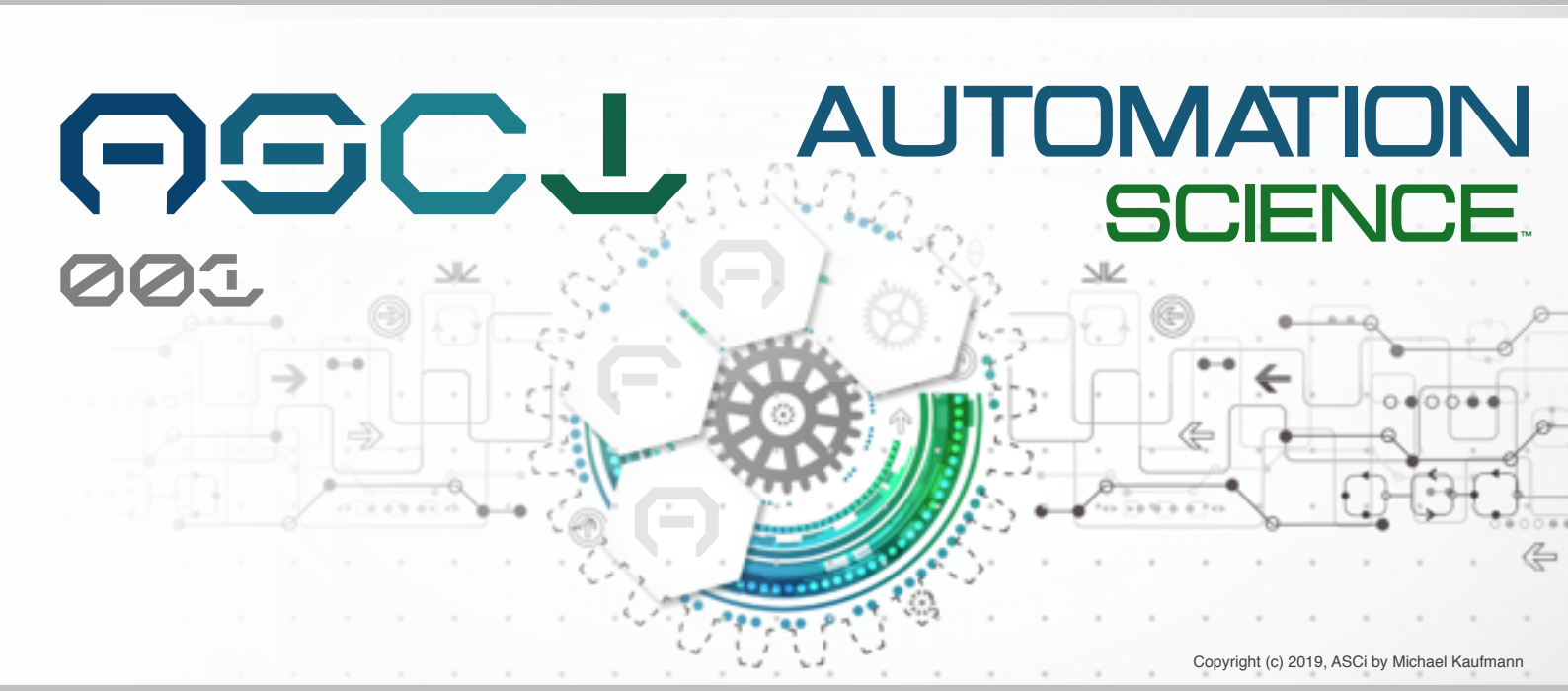



Copyright (c) 2019, ASCi by Michael Kaufmann

# Vorwort

## Über Automation Science

Was ist das Automation Science™ eigentlich? Nun, dieses kleine Format hieß früher einmal „Automation für Arme“ und entstand eher aus einer Laune und gleichzeitigem Interesse heraus.

Viele Gespräche die ich mit Kunden oder Kollegen geführt habe, zeigten mir, dass es für viele Informationen kein eigenes Bild (im Kopf) gibt, auf das direkt Bezug genommen werden kann, wenn es um Technik geht. Oft wurde ich zu tiefergehenden, aber auch Einzelheiten befragt, die nicht verstanden wurden oder schlicht die Vorstellung fehlte. Auch hielt sich, bei vielen meiner Kollegen mit Fachausbildung, dass Wissen - in den Tiefen des Verstehens - doch etwas begrenzt. Es kann sich nun einmal nicht Jeder/e, mit allem befassen. Nun genau ab da fing es an, denn daran wollte ich etwas ändern und habe mich auf die Themen bezogen, die gerade vor kurzen aktuell waren. So entstand eine Dokumentation und Leitlinien zu einer Vielzahl von unterschiedlichen Themen (Software Hacking, Viren- und Trojaner, ReEngineering, Hardware Tipps, Beispiele für Automaten und einiges andere) die ich etwas spielerisch *umschrob*, aber immer mit Fokus auf eine einfache Erklärungsweise wie auch die Bebilderung.

Seit 2018 schreibe ich an Dokumentationen, Anleitungen und des öfteren habe ich Anfragen von Agenturen, Zeitschriften und Verlagen bekommen. Es ist jedoch etwas anderes für ein Blatt zu schreiben; als locker und unverblümt aus einen selber heraus. Weshalb ich auf diese Angebote, erst einmal verzichtete. Dies lag schon alleine daran, dass ich nicht des Schreibens willen, sondern aus philosophisch-technischer Bestrebung heraus, versuche die Zusammenhänge zu erklären; weshalb ich mich auch 2019 dafür entschlossen habe, meine Arbeiten im Hintergrund mehr zu benennen und das Format


Copyright (c) 2019, ASCi by Michael Kaufmann

(hier) zu Automation Science *(kurz: ASCi)* umzubenennen. Alle Arbeiten und Denkprozesse in dem Bereichen des Testings und Automaten, geht nicht zuletzt auf meine Arbeiten als Speaker und Philosoph zurück und wie ich selber gerne zu sagen pflege: „Ein guter Philosoph, fängt immer beim Worte an“ - und da geht es auch schon los. Das ein Wort wie Qualität heute so sehr gedehnt; von den Meisten absichtlich *falsch* verstanden und gleichzeitig auch unmittelbar missbraucht wird - hätte sich selbst Aristoteles, nie zu träumen gewagt. Doch was ist nun Automation genau genommen? Und genau dort fängt es an…

## Motivation

Eben so beiläufig wie ausgibt, nutzen wir ein Wort wie *Automation;* jegliche, und doch, ohne uns bewusst zu machen, unter welchen Aspekten es im eigenem und engerem Sinne, es überhaupt zu nutzen ist. Wie in allen Sprachgebräuchen; geht Sinnhaftigkeit erst, mit ihrer Häufigkeit und Anwendung verloren. Wann immer, eine unzureichend verstandene Maßlosigkeit wie: „das geht ganz *automatisch*“, durch Ihre Verwendung verloren geht, braucht es einer neuen Idee. Sie besteht meist nicht aus dem Verstand eines neuen Maßes, eher um neues zu predigen; mehr noch so zu tun, das Bestehende durch sich selbst, besser verstehen zu lernen. Und so sehe ich es als eine wichtige Aufgabe an, verstehen und das Dahinter, wieder mehr in den Fokus zu setzen. Auch um das Denken wieder zu schärfen und gleichzeitig, die Angst vor der Technik zu verlieren, um sie besser verstehen, mehr noch; sie besser betrachten zu können.

## Publikation

Ich habe beschlossen dieses Format (ASCi - Automation Science*)* ab der heutigen Ausgabe, nicht mehr vorrangig für Firmen-Kollegen und -Kolleginnen bereit zu stellen, sondern über eine öffentliche Publikationsform (Feed & Website). Dies erleichtert die Weitergabe, verkürzt zu gleich die eMail Fluten und ermöglicht es mir auch, auf anderen Wegen, Feedback einzuholen. Bis Ende August 2019 werde ich noch an den Vorbereitungen für eine Seite sitzen, worüber diese Beiträge auch mittels Feed abruf- und herunterladbar sind. Alle Beiträge werden auf Github hinterlegt und auch über die Akademie: LAoP (Liberum Academy of Philosophy) später abrufbar und per Download bereitgestellt.

Mit freundlichen Grüßen

Michael Kaufmann



Copyright (c) 2019, ASCi by Michael Kaufmann


# Für mehr Sicherheit durch Two-Factor-Authentication

## Doch wie sicher ist die Methode wirklich bei Angriffen durch Man-in-the-Middle oder Phishing?

Ich habe mich dazu entschieden, dies einmal zu testen und habe dafür in einem Live-Szenario, ein Hacking Framework in Anwendung gebracht. Da dies keine Anleitung als Selbstversuch darstellt, gehe ich nur auf das eigentliche Vorgehen ein, nicht auf die direkt verwendeten Tools, der Umgebungen oder die Benutzeraccounts. Dabei ziele ich auf das Verfahren, weniger auf die Anwendung ab, die ich dabei kurz beschreibe, um zu demonstrieren, wie ein solcher Angriff abläuft.

### DISCLAIMER

Ich weis darauf hin, dass dieses Dokument (AfA002) keine Anleitung zum Selbstversuch darstellt! Es ist verboten, fremde Accounts und Tools in den Einsatz zu bringen oder diese ungefragt zu verwenden, um Identitäten, Zugänge fremder oder Nutzsysteme ohne Einverständnis der Nutzer und-, oder derer Besitzer selbst; anzugreifen, zu übernehmen oder zu Gunsten weiterer Delikte oder Straftaten zu verwenden. Dieses Dokument dient allein der Verdeutlichung und Aufklärung. Das Einsetzen von Hacker-Tools an sich, ist in Deutschland unter Strafe gestellt. Weiteres regelt das StGB: § 149, § 202, § 202a, § 202b, § 202c, $ 206


Copyright (c) 2019, ASCi by Michael Kaufmann

Damit soll auch klar werden, wie am schnellsten auf Daten Fremder, zugegriffen werden kann. Auch möchte ich damit zeigen, dass nicht *all-zu-technisch* versierte Menschen, ein solches Angriffsszenario durchführen können. Um an Kontodaten oder an Social Accounts zu kommen, werden wir sehen, dass uns eine 2FA hierfür eher egal sein kann. Wie umsichtig die meisten mit Ihren eigenen Zugangsdaten umgehen und wie wenig sicher sie letztlich sind, zeigen auch die (zuletzt) in den Medien aufgegriffenen Geschehnisse.

So wurden ca. 2,2 Milliarden Zugangsdaten (lauf dem Plattner Institut) von NutzerInnen in fünf darauf folgenden *Collections* gestohlen. Ob es sich nun um das absichtliche stehlen von Privatdaten im großem Stiele - wie etwas bei Equifax - handelt oder um Massen-Doxxing, bei dem es um das unerkannte eindringen in Systeme und das reine sammeln von Privatdaten geht. Die Angriffe und deren Szenarien sind stets die selben und auch erfolgreich.

Schon lange geht es nicht mehr um das besitzen von eigentlich tiefen Kenntnissen von Computersystemen. Wie auch beim Promi-Doxxer: 0rbit es sich zuletzt zeigte, ist ein tiefes Fachwissen nur von Nöten, wenn eigene Software und Strategien erarbeitet werden sollen. Da Cracker schon sehr früh damit anfingen Werkzeuge für erkannte Angriffe zu entwickeln, braucht es heute, kaum noch höheres Wissen um Szenerien eines Angriffes, voll automatisiert auszuführen.

Schauen wir uns daher in Folge eine Szenario an, bei dem ich mit Erfolg versucht habe, einen direkten Zugriff auf ein Soziales Netzwerk zu bekommen.

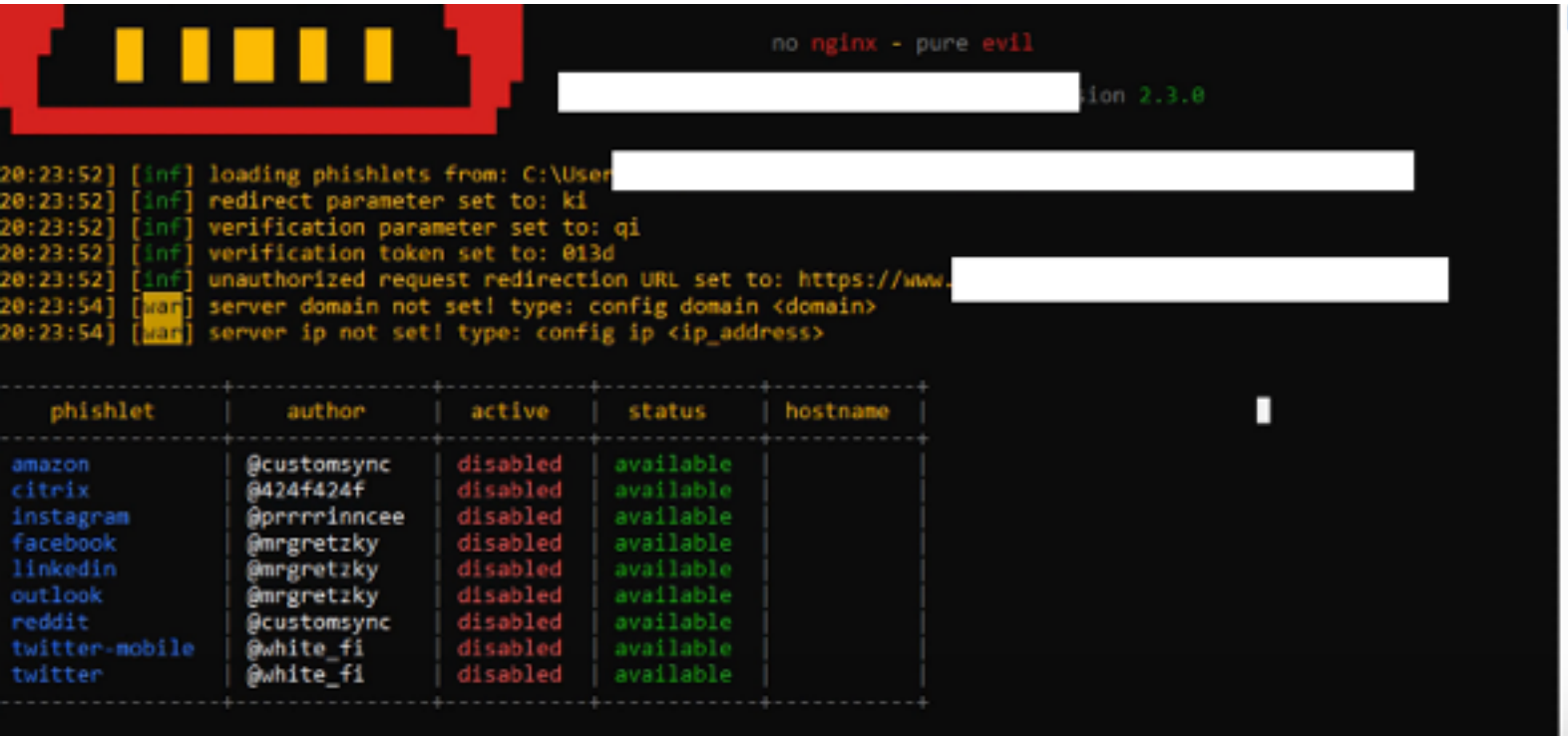
## Aufbau und Funktionsweisen

Die Methoden der meisten Angreifer-Tools sind Attacken, wie die, die durch Man-in-the-middle durchgeführt werden. Das es viele solche Szenarien gibt, eine solche Prozedur durchzuführen, sind diese Toole meist auch erweiterbar. Heißt: sie sind durch zusätzlichen Code ausbaufähig und aufrüstbar.

Diese werden als Hacking- oder Crack-Frameworks bezeichnet. Sie können ebenfalls, bestehende Tools einbinden um sie nacheinander oder gleichzeitig ansteuern zu können.


Copyright (c) 2019, ASCi by Michael Kaufmann

Das von mir in diesem Zusammenhang genutzte Hacker-Framework, hat schon einiges an Szenarien installiert. So benötige ich für einen einfachen Angriff, keine großen Erweiterungen und auch *eigentlich* kein Know-how, um einen Angriff auszuführen.




Screenshot mit Angriffsvektoren. Angaben der Umgebung und weitere Informationen wurden ausgeblendet

Die jeweilig nutzbaren Angriffsvektoren werden hier als **phishlet** (=phishing; also die Szenarien zum abgreifen der Daten) bezeichnet. Diese lassen sich für später auch mit gezielten Angriffe und weiteren phishlets erweitern.

## Allgemeines

Um einen Angriff ausführen zu können, benötige ich nun einen Server der möglichst direkt im Internet angesprochen werden kann, auf dem sich das Opfer letztlich anmeldet um die eigenen Benutzerdaten einzutragen. Dies kann auf unterschiedlichste Weise funktionieren. Zum Beispiel über einen Schadcode (Java-Script, Flash) in Add-Werbung oder Bannern auf Web-Seiten.

Auch bestehende Codebausteine zu Benutzerbezogenen Aufzeichnungen (Tracking: speichern der Bewegungen und von Aufrufen usw.) auf Websites, lassen sich hier hervorragend ausnutzen und umbiegen.

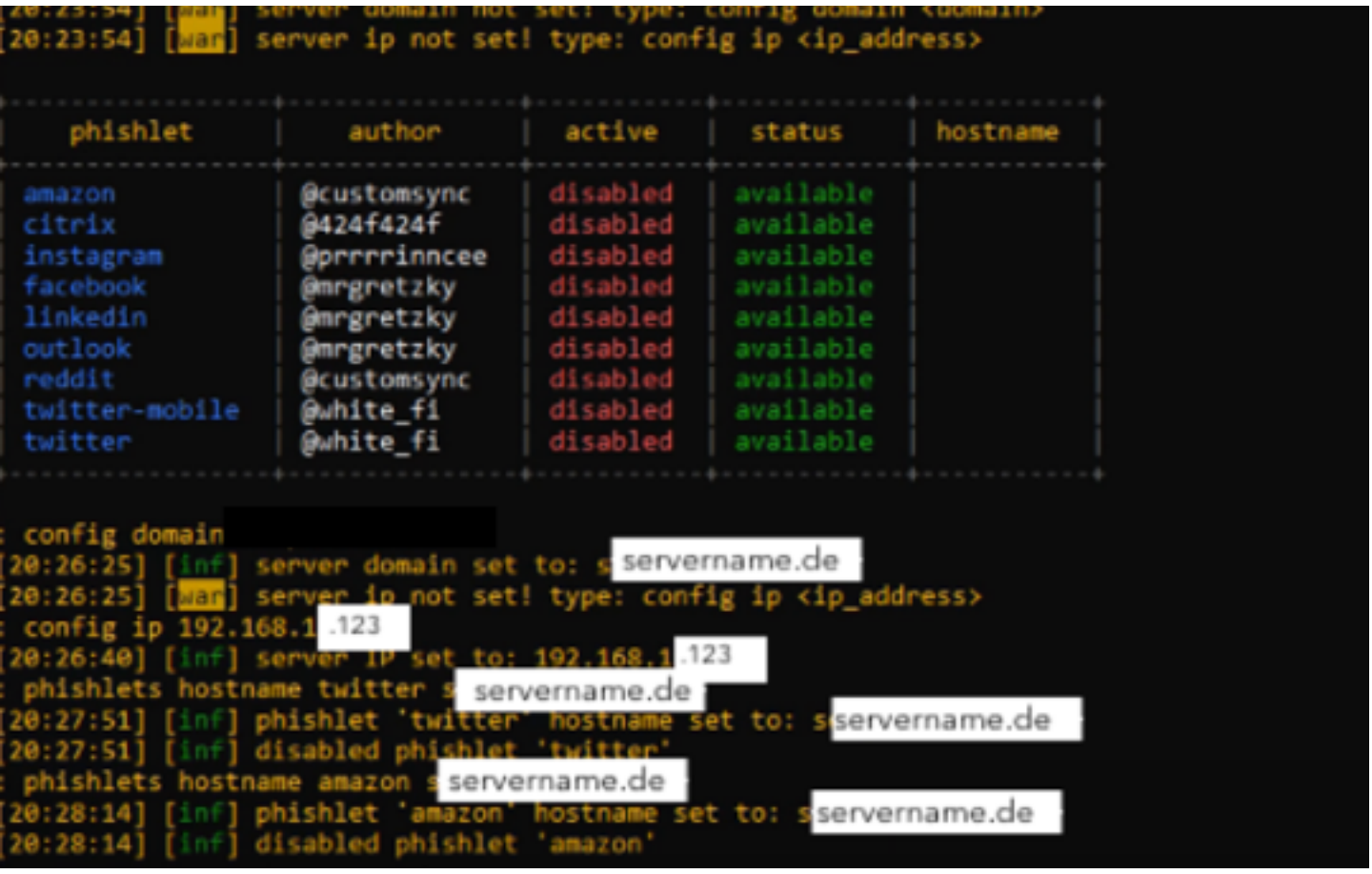

Copyright (c) 2019, ASCi by Michael Kaufmann

In meinem Beispiel möchte ich einen Angriff per eMail durchführen, bei dem das Opfer auf eine Link klickt. Dieser führt zu einem von mir (meist von Angreifern gekaperten) Server. Dieser leitet wiederum zu vielen anderen Servern weiter, zu dem am Ende ein Server mit einer F3ZZ Domain steckt. Das Opfer bemerkt dabei nicht, dass es auf einer fremden Website landet, als der, auf der sie sich augenscheinlich gerade befindet.

F3ZZ bedeutet in Übrigen, dass ein Zeichen einer anderen Sprache, innerhalb einer Domain auftaucht und dort absichtlich versteckt wurde. So lassen sich viele Domains fälschen. Mit einem freien SSL Zertifikat wird die Website, dann sogar HTTPS verschlüsselt und sieht sicher für jedes Opfer aus.

## Los geht es

Als erstes lasse ich mal eine Verbindung zu meinen Rechnern über die IP (der Hintergrund der Datenübermittlung ist Verschlüsselt und wird über mehrere Proxies ins Ausland weitergeleitet) herstellen.



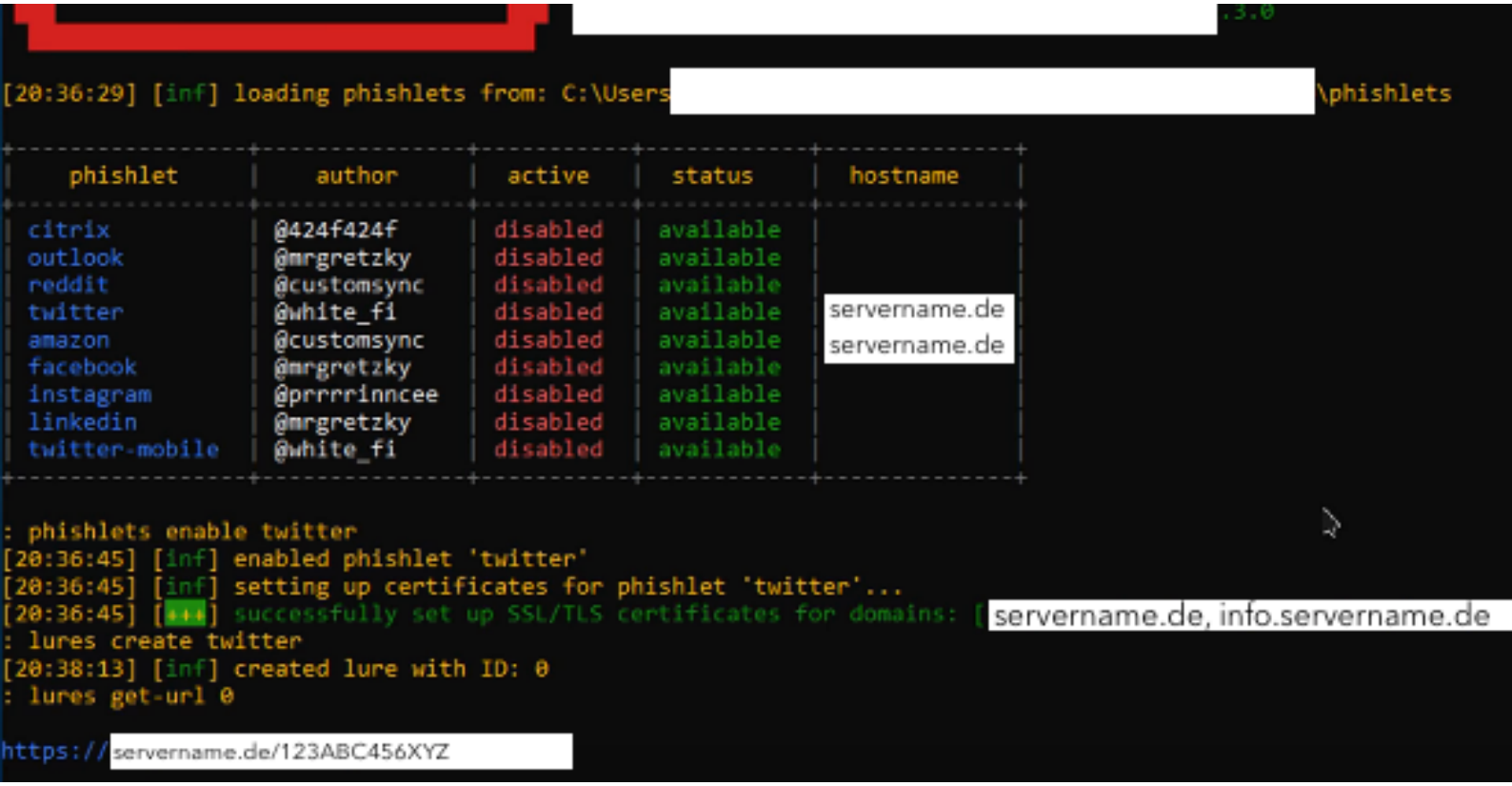

Dann benötige ich natürlich noch die Domain meines *gehackten* Servers, über die das Opfer gelangen soll.


Copyright (c) 2019, ASCi by Michael Kaufmann

**INFOS**

Die hier eingetragen Domain und eigene IP-Adress ist beispielhaft verwendet und wurden rein aus Dokumentationsgründen überschrieben. Die Domain wurde in diesen Szenario nicht verwendet noch angegriffen!

Sind die *phishlets* eingetragen und der Server aktiviert, werden die verwendeten Attacken nun auch in der Tabelle angezeigt.




Ich möchte nun eine Attacke ausführbar machen und starte das phishlet *twitter.* Um zusätzlich als Man-in-the-middle zu agieren, wird meine Verbindung zum Server, noch einmal über ein SSL/TLS-Zertifikat abgesichert und verschlüsselt.

Nach dem nun das Framework die Session aufgebaut hat, lasse ich mir eine Schlüssel-URL erzeugen, die ich später in einer eMail einbauen kann, um mein Opfer dazu zu bringen, diese URL anzuklicken.

Hier als Beispiel Schlüssel-URL als https://servername.de/123ABC456XYZ angegeben.

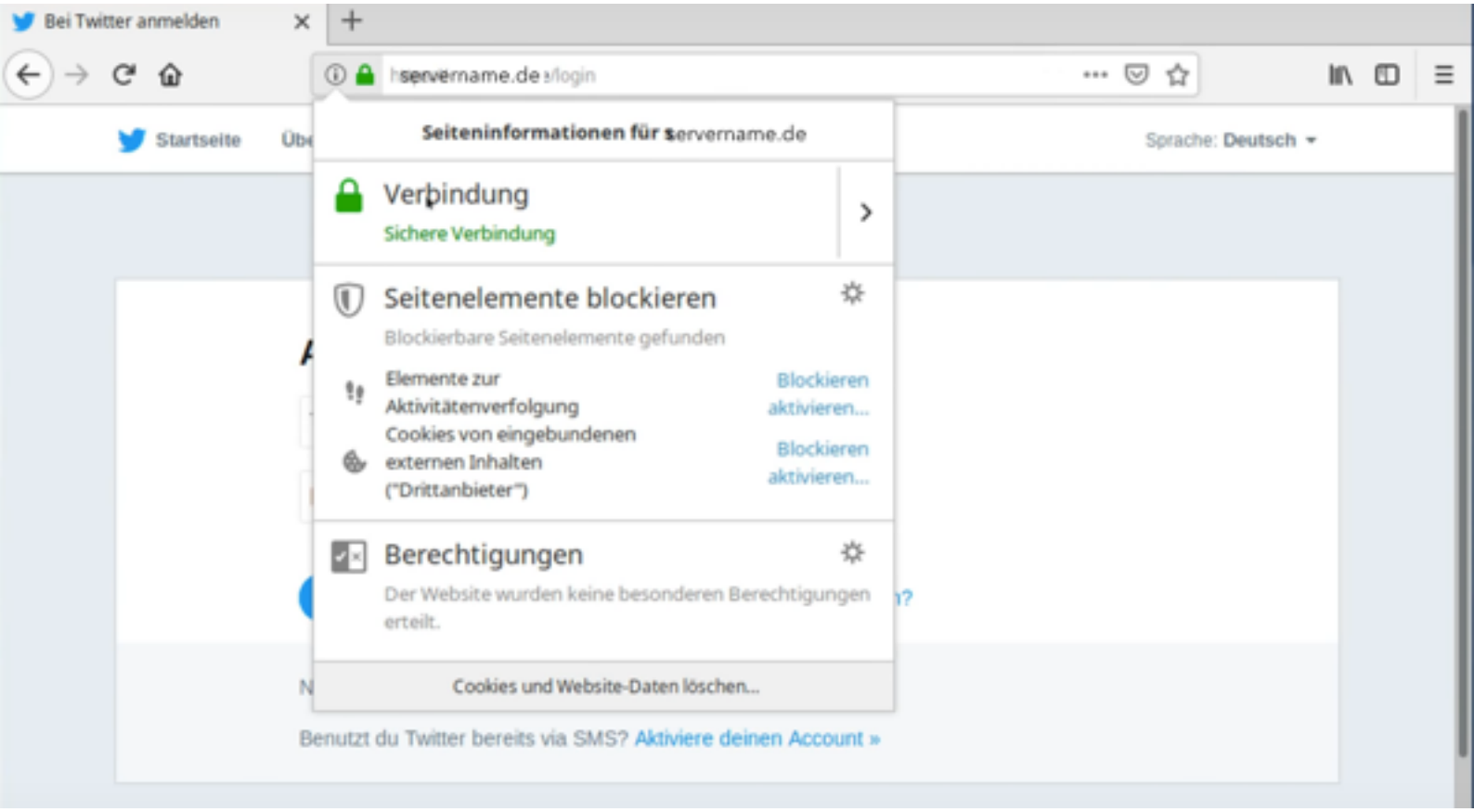

Copyright (c) 2019, ASCi by Michael Kaufmann

# Phishing me

Das Prinzip von phishing Mails hat sich seither eigentlich kaum verändert. Wir können die URL natürlich auch sehr weit treiben und sie in Artikeln verstehen uns sonst etwas. Natürlich könnten wir sie auch bei Gewinnspielen oder Ade-Werbeanzeigen unterbringen. Denn tatsächlich werden diese Angaben von den Werbebetreibern der Server nicht überprüft.

**Kommen wir aber zurück zu unseren Angriff…**

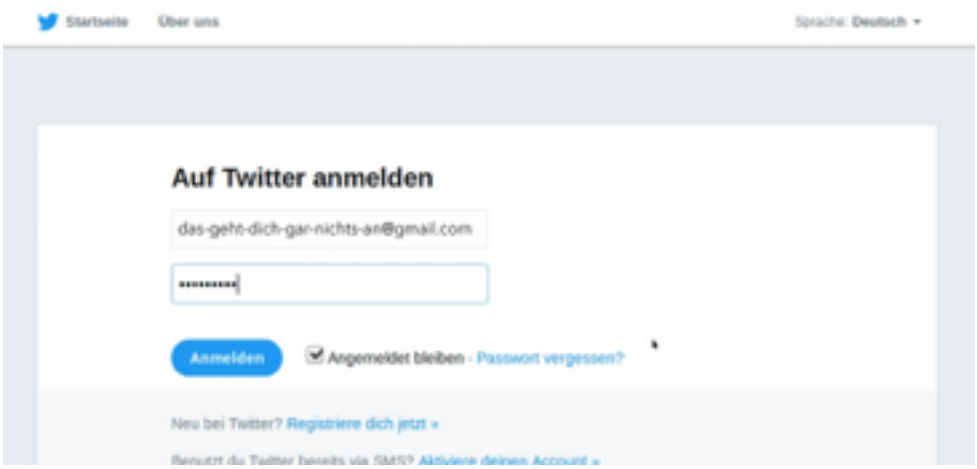
Ich spiele nun das Opfer und klicken auf den Link in der fake-Mail. Nach dem Aufrufen, werden wir überrascht sein, denn auch die Verschlüsselung sieht richtig aus.




Einzig und allein unsere Domain würde uns verraten. Dies liegt aber daran, dass wir uns eben keine F3ZZ Domain zugelegt haben.


Copyright (c) 2019, ASCi by Michael Kaufmann

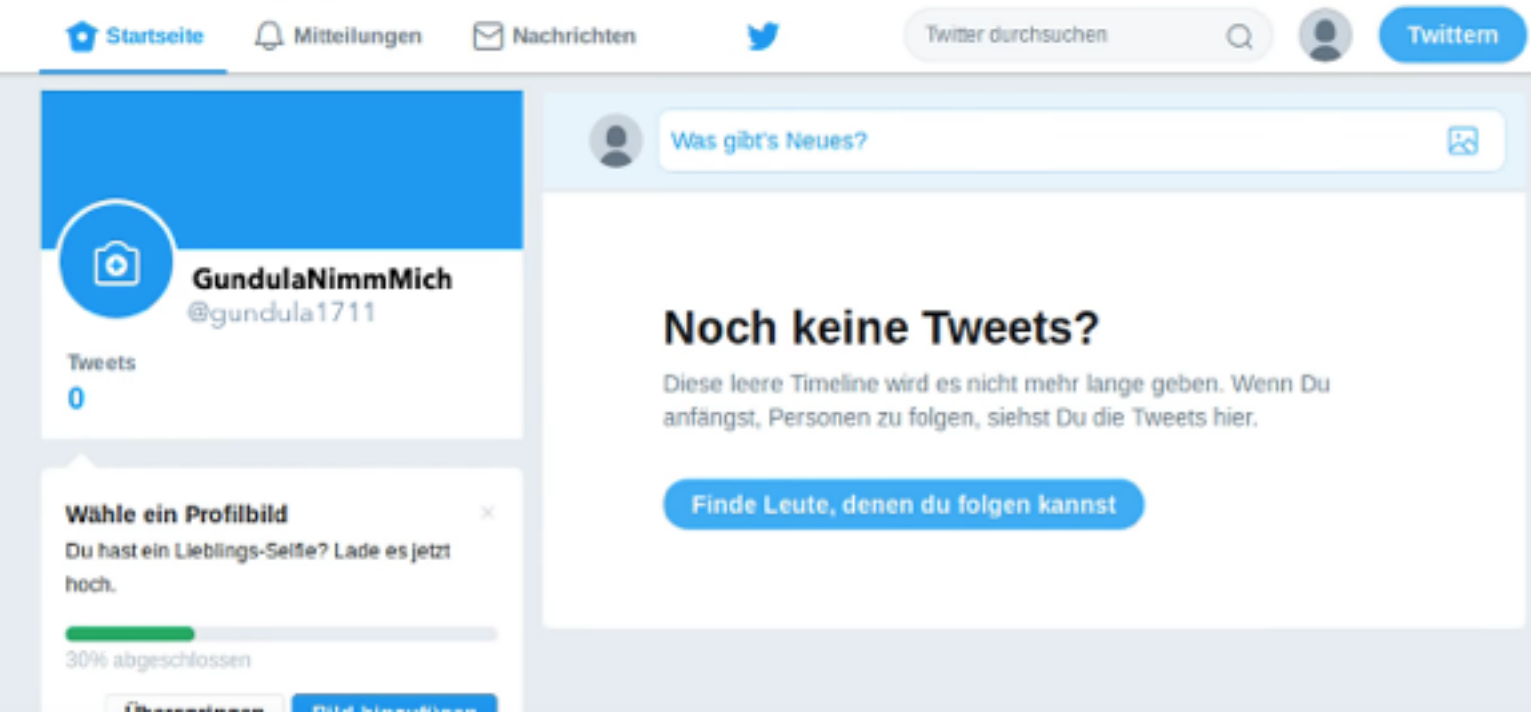
Ist dem Opfer nichts weiter aufgefallen, dann brauche ich nur noch darauf zu warten, bis es seine Daten auf dem gehackten Server eingegeben hat.





Nach drücken des Anmeldebuttons wird eine Weiterleitung zum Twitter-Server durchgeführt und die Daten werden direkt als Login übergeben.

**Erst jetzt wird die 2FA ausgelöst, doch nun ist es schon zu spät!**



In der Zwischenzeit, habe Ich die Daten unseres Opfers mitgeschnitten und nicht nur die Anmeldedaten unverschlüsselt abgegriffen. Was ich zusätzlich noch bekommen habe; sind all seine Schlüssel, in dem sich auch die Cookies befinden.

Damit sind alle Informationen für mich nur noch als Speicherspaß anzusehen. Für mich ist jedoch der Cookie deutlich interessanter, da ich damit - direkt - und ohne weitere Angaben von Daten von meinem Rechner aus, an Twitter anmelden kann.

## Cookie auslesen

Um den Cookie meines Opfers auszulesen, laden ich einfach die letzten Session:

| phishlet | author | active | status | hostname |
|---|---|---|---|---|
| amazon | @customsync | disabled | available | |
| facebook | @mrgretzky | disabled | available | |
| outlook | @mrgretzky | disabled | available | |
| twitter | @white_fi | enabled | available | |
| citrix | @424f424f | disabled | available | |
| instagram | @prrrrinncee | disabled | available | |
| linkedin | @mrgretzky | disabled | available | |
| reddit | @customsync | disabled | available | |
| twitter-mobile | @white_fi | disabled | available | |

: sessions

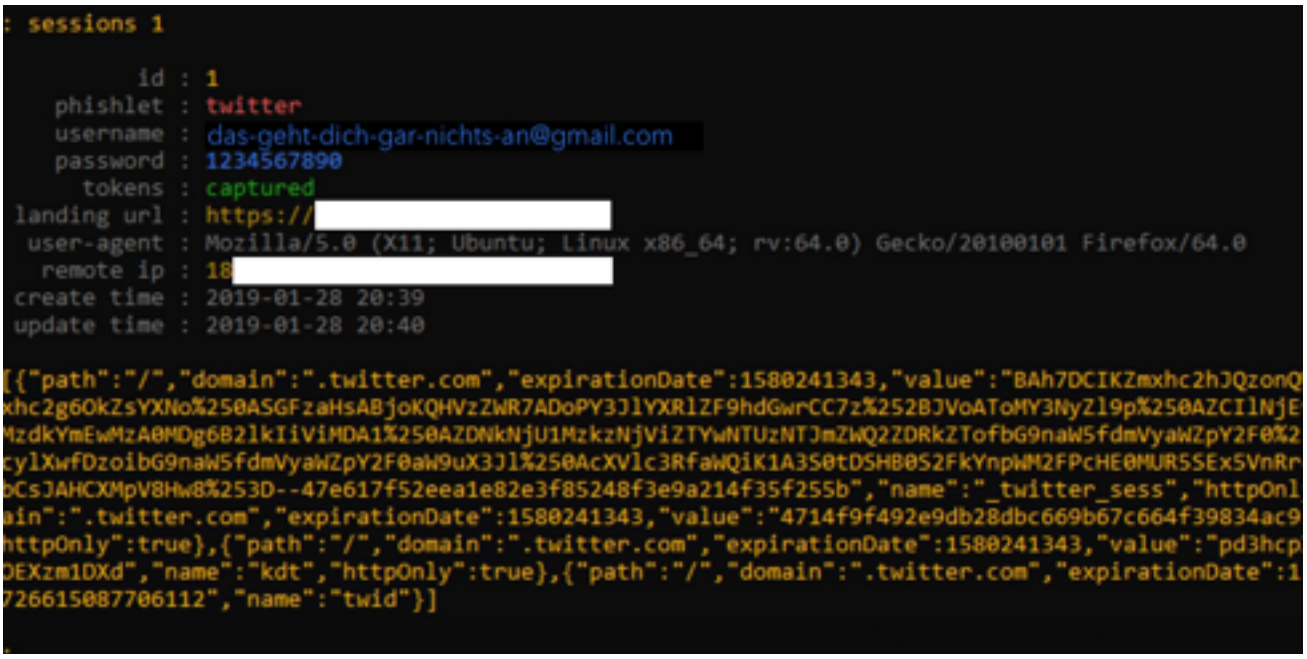
| id | phishlet | username | password | tokens | remote ip | time |
|---|---|---|---|---|---|---|
| 1 | twitter | das-geht-dich....@gmail.com | 1234567890 | captured | | |

Nach dem ich die Session geladen habe, kann ich nun den Cookie ausgeben lassen. Ich kopiere mir einfach den Inhalt des Cookies und kann Ihn über den Browser übergeben. Natürlich werden alle wissen, das Angreifer, immer auch Spuren des eigenen Rechners hinterlassen. Daher werden meist Proxy-Server oder Cloud-Browser und / oder weitere Dienst genutzt, um dies zu verschleiern. Diese Dienste benenne ich hier nicht weiter und sind für uns auch nicht wirklich von Interesse, da ich den Angriff hier nur als Demo darstelle und keine realen Personen oder Accounts fremder angegriffen und bestohlen werden.

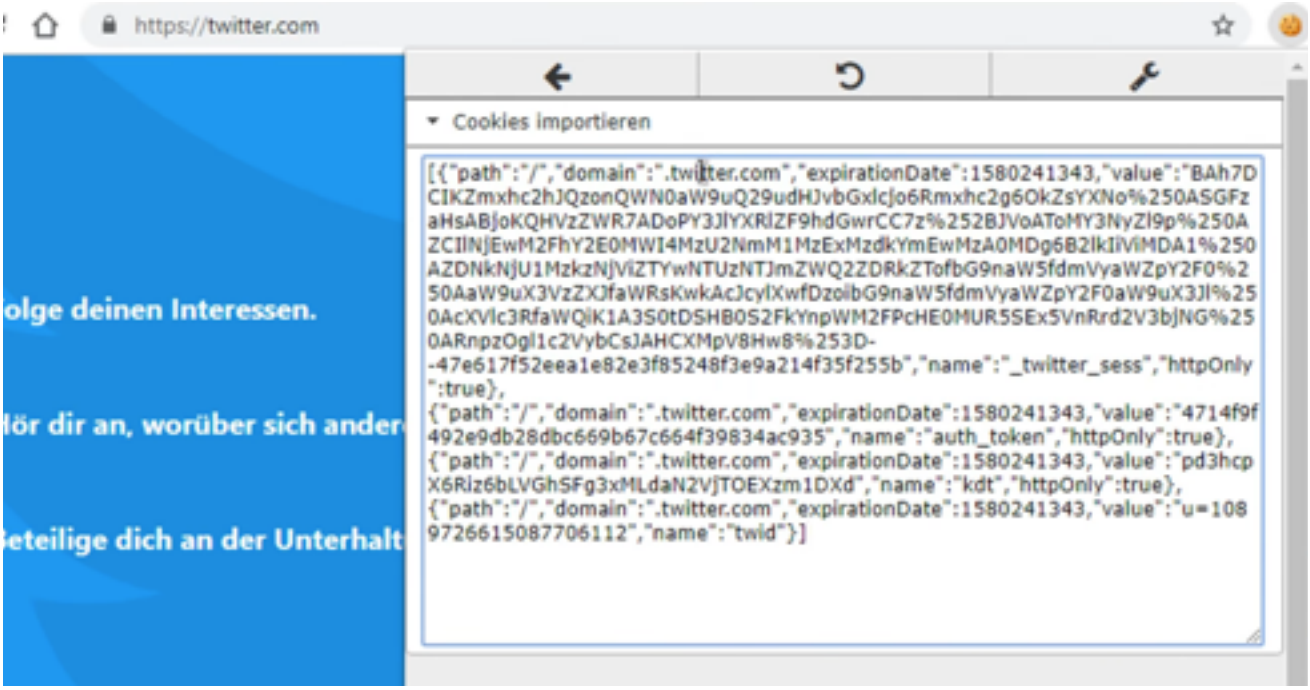

Copyright (c) 2019, ASCi by Michael Kaufmann

# Login auf Twitter

Da ich nun den Cookie unseres Opfers kenne, kann ich mir diesen anzeigen lassen um Ihn mir zu kopieren.



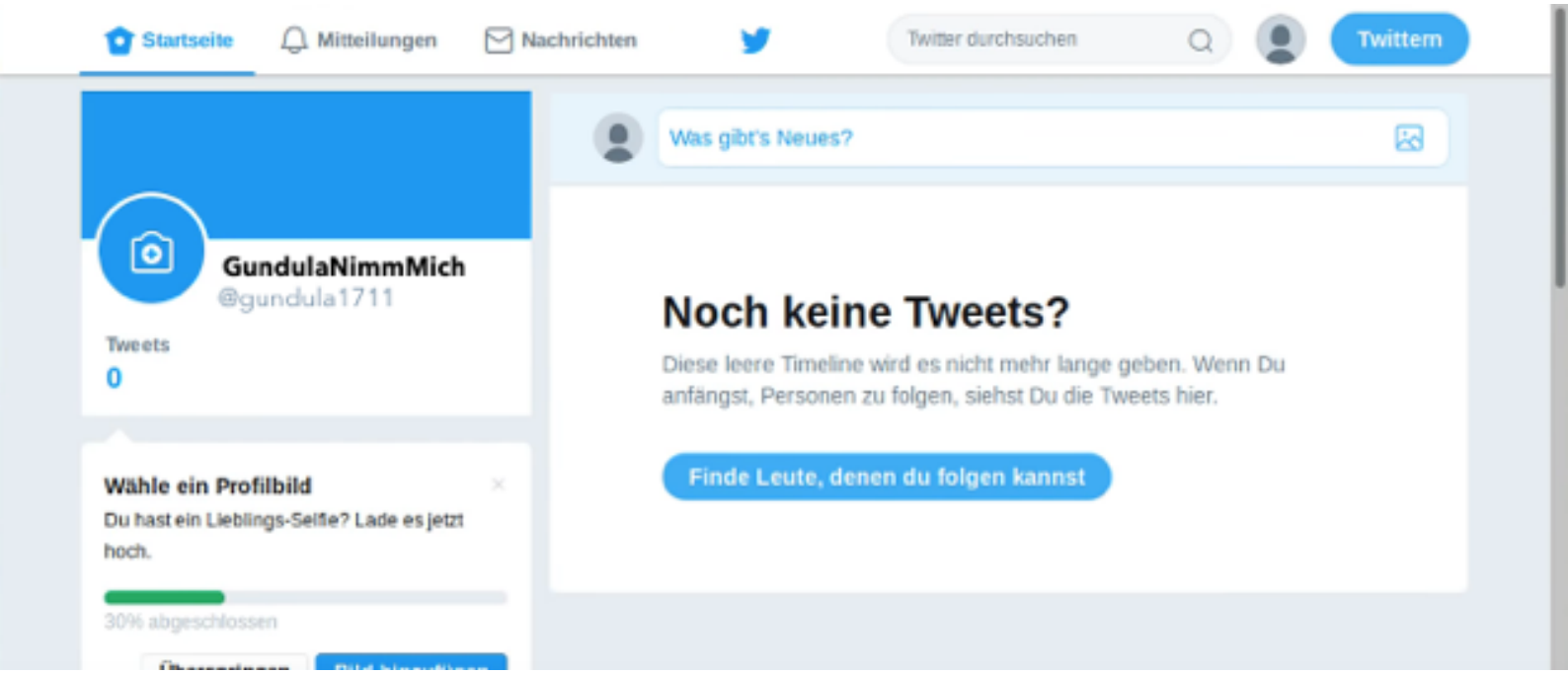

Das Übertragen eines bestehenden Cookies in den Browser kann ich einfach über ein weiteres PlugIns erledigen:





Copyright (c) 2019, ASCi by Michael Kaufmann

Ist der Cookie einmal übergeben, brauch nur noch die Website aktualisiert werden und ich bin angemeldet, mit den Daten unseres Opfers.




Ich kann nun alle Angaben, Daten, Informationen, Bilder, Videos und mehr sammeln oder im Namen einer anderen Person schreiben. Es wird deutlich unangenehmer, wenn ich einen Amazon oder E-Bay Account finde. Es gibt sicher genug Möglichkeiten sich gegen solche Angriffe zu schützen. Zum Beispiel sollten deine Accountdaten verschlüsselt und mit einem speziellen Tool gesichert werden. Auch sollten deine Passwörter mindestens 21 Stellen haben.

## Fazit

Es ist recht einfach Daten anderer Personen abzugreifen und es lässt sich in nur wenigen Schritten (auch ohne Fachkenntnisse) von einem Angreifer aus umsetzen. Der Schaden kann enorm für die potenziellen Opfer sein. Eine 2FA ist sicherlich sehr nützlich, bringt jedoch bei Phishing-Angriffen keine Punkte. Die 2FA-Fragen oder direkte Handy-Bestätigung, hilft hier nicht weiter, da sie erst nach einem Angriff in ausgeführt werden, dann ist es meist schon zu spät.

Autor: Michael Kaufmann - 04.01.2019


Copyright (c) 2019, ASCi by Michael Kaufmann