# Lehren aus dem Politiker-Hack

## Eigene Onlinekonten gegen Datenklau absichern

**Intime Daten hunderter Prominenter und Politiker standen frei zugänglich im Netz. Dabei wäre der Schutz vor einem solchen Angriff recht einfach gewesen. Das sind die wichtigsten Schritte zum Absichern der eigenen Onlinekonten.**

**Von Fabian A. Scherschel**

Ein zwanzig Jahre alter Schüler aus der hessischen Provinz hat private Daten hunderter deutscher Politiker und Prominenter im Netz veröffentlicht und die Republik in Aufruhr versetzt. Der Fall des Schülers, der aktuellen Erkenntnissen nach keine besonderen Hacker-Fähigkeiten besitzt, zeigt, wie einfach es ist, zum Opfer einer solchen publikumswirksamen Enthüllung zu werden. Es müssen gar nicht immer die Geheimdienste aus Russland oder den USA beschworen werden, denn wie es aussieht, brauchte der Schüler nicht viel mehr als einen guten Sinn für Recherche, viel Fleiß und etwas Zeit, um für ein paar Tage der meistgesuchte Hacker Deutschlands zu werden – und nebenbei noch vielen Menschen das Leben schwer zu machen.

Er hatte die Telefonnummern, Personalausweis-Scans und Adressen seiner Opfer wohl einfach aus schlecht gesicherten Konten diverser Online-Dienste zusammengeklaut. Wahrscheinlich reichte der Zugang zum Mailkonto eines Bundestagsabgeordneten, um die Daten vieler Parteikollegen zu sammeln. So schaffte es der hessische Schüler schließlich sogar, an die Handynummer von Martin Schulz zu kommen. Geübt hatte er wohl jahrelang in der YouTuber-Szene. Das Twitter-Konto, von dem er seine Enthüllungskampagne startete, hatte er vor Jahren einem YouTuber abgenommen, der sein Geld mit dem Trollen von Minecraft-Spielern verdient.

Allerdings interessierten die Angriffe und das Offenlegen privater Informationen von YouTubern jahrelang kaum jemanden. Solche in der Szene auch als Doxxing bezeichneten Aktionen sind relativ üblich und kaum einer der technikversierten Videoproduzenten traut der deutschen Polizei zu, solche Angriffe aufzuklären. Mit Recht, muss man sagen – wenn man sich das tollpatschige Verhalten deutscher Sicherheitsbehörden in diesem Fall anschaut – allen voran des Bundesamtes für Sicherheit in der Informationstechnik, BSI. Erst als die Presse vom Datenklau Wind bekam und ihn publik machte, erwachten die Behörden aus dem kollektiven Winterschlaf und fanden den hessischen Schüler innerhalb von zwei Tagen. Der geständige Täter hatte sich offenbar nicht besonders gut versteckt. Zu diesem Zeitpunkt hatten mehrere YouTuber der Presse bereits Interviews gegeben und sich damit gebrüstet, zu wissen, wer der Täter sei.

Um derartige Doxxing-Fälle in Zukunft zu verhindern, muss man die eigenen Online-Konten vor Übergriffen schützen. Dafür gibt es ein paar einfach umzusetzende Punkte, dir wir im Folgenden zusammengefasst haben.

### Passwörter sicherer machen

Der wichtigste Schutz vor Doxxing-Angriffen besteht darin, die eigenen Passwörter sicherer zu machen. Dabei ist es gar nicht nötig, alle Logins bei allen Webseiten und Programmen zu ändern. Aber identifizieren Sie die kritischsten Angriffspunkte und sorgen Sie dafür, dass Sie für diese besonders begehrten Ziele gute und einzigartige Passwörter verwenden. Je länger und zufälliger ihre Passwörter sind, desto besser. Verwenden Sie auf keinen Fall Begriffe oder Phrasen, die in einem


Unter den geleakten Daten befand sich auch die Handynummer des ehemaligen SPD-Kanzlerkandidaten Martin Schulz.

Wörterbuch zu finden sind und lassen Sie auf jeden Fall die Finger von Geburtsdaten, Haustiernamen und ähnlichen leicht zu erratenden Fakten. Ausführliche Tipps zum Erstellen guter Passwörter finden Sie zum Beispiel in den Sicherheits-Checklisten aus c't 20/2018. Die Listen kann man in einer Kurzfassung auch gratis herunterladen (siehe ct.de/yzc8).

Am besten ist es, wenn Sie kein einziges Passwort mehrmals verwenden. Auf diese Weise bleibt ein Einbruch bei einem Dienst auf diesen beschränkt und Sie verlieren nicht auch noch die Daten von anderen Seiten, bei denen Sie dasselbe Login verwenden. Natürlich kann man sich alle diese unterschiedlichen Passwörter unmöglich merken und sie aufzuschreiben kann ganz andere Angriffsszenarien eröffnen.

Es empfiehlt sich deswegen, einen Passwortmanager zu verwenden. Solche Programme nehmen Ihnen oft auch das mühsame Erstellen der einzelnen Passwörter ab und können mit einem einzigen Master-Passwort gesichert werden. Das sollte allerdings sehr lang und kompliziert sein – immerhin müssen Sie sich dann aber nur eins merken. Manche Passwortmanager lassen sich auch per Fingerabdruck entriegeln, was die alltägliche Nutzung erträglicher macht.

Wo es geht, sollten sie Zwei-Faktor-Authentifizierung aktivieren. Bei diesen Systemen wird neben dem Passwort beim Login zusätzlich ein Einmal-Code abgefragt, den Sie zum Beispiel per App auf einem Smartphone oder per SMS erhalten. Das macht etwas mehr Mühe beim Login, erschwert Hackern den Angriff allerdings kolossal. Mindestens beim Online-Banking und dem E-Mail-Postfach ist Zwei-Faktor-Anmeldung unumgänglich.

## Besonderer Schutz für das E-Mail-Konto

Ob bei gezielten Angriffen auf Firmen oder nach einer Trojaner-Infektion aus massenweise versandten Spam-Mails, meist haben es Angreifer auf das Mailkonto des Opfers abgesehen. Denn das Mailkonto ist der neuralgische Punkt des digitalen Lebens: Hat der Angreifer hier Zugang, kann er leicht herausfinden, welche Webseiten und Dienste das Opfer nutzt. Dabei muss er nicht einmal die Passwörter für diese Dienste kennen, denn die Mailadresse fungiert in den meisten Fällen als Login und damit kann


**Über eine Art Adventskalender hatte der Täter die Daten auf Twitter veröffentlicht. Sie standen wochenlang frei verfügbar im Netz.**

er sich auch gleich das Passwort zurücksetzen lassen. Von einem Mailkonto lassen sich also fast alle Aspekte der digitalen Online-Identität einer Person kontrollieren.

Verwenden Sie deswegen unbedingt ein besonders robustes Passwort für Ihre Mailkonten. Schalten Sie wenn möglich das Nachladen externer Bilder oder gar jegliche HTML-Darstellung in Ihrem Mailprogramm ab. Lassen Sie äußerste Vorsicht walten, wenn Sie E-Mails mit Links oder Anhängen bekommen – vor allem, wenn Sie diese nicht erwarten. Vor einem Klick auf einen Link oder dem Öffnen eines Anhangs sollte man im Zweifel auf einem anderen Kanal, etwa am Telefon, nachfragen, ob die Mail auch wirklich von dem Absender kommt, der im Mailprogramm genannt wird. Diese Zeit sollte man sich nehmen, schließlich gelangen Trojaner dieser Tage oft über manipulierte Word-Dokumente auf Computer.

## Software aktuell halten

Nicht nur Onlinedienste, auch lokale Geräte muss man schützen. Neben einem funktionierenden Virenscanner – etwa dem in Windows 10 standardmäßig enthaltenen Windows Defender – ist es unabdingbar, wo es nur geht die verwendete Software aktuell zu halten. Das Betriebssystem, alle Browser und auch etwaige lokale Mailprogramme sollten alle selbstständig Updates erhalten. Wer einen PDF-Reader von Adobe oder Office-Software verwendet, sollte auch hier stetig für Aktualisierungen sorgen. Die beste Verteidigungssoftware nutzt nämlich nichts, wenn im Betriebssystem oder in kritischen Programmen bekannte Lücken klaffen, die ein Angreifer ausnutzen kann.

In diesem Zusammenhang sei auch darauf hingewiesen, dass neue Software nur aus vertrauenswürdigen Quellen installiert werden sollte. Also am besten aus offiziellen App-Stores des Betriebssystemherstellers oder von der Webseite des Herstellers. Am besten überprüft man zweimal, auf welcher Webseite man auf einen Download-Link klickt. Nicht wenige Opfer holen sich den Trojaner selbst auf den Rechner, nachdem sie unter einem Vorwand auf fingierte Webseiten gelockt wurden.

Wer diese Hinweise befolgt, ist natürlich auch nicht komplett davor gefeit, seine Daten im Twitter-Adventskalender eines hessischen Schülers wiederzufinden, aber es macht eine solche Katastrophe deutlich unwahrscheinlicher. Selbst wenn die Vorsorge nur den Unterschied dazwischen macht, ob persönliche Daten aus dem Adressbuch eines Kontakts geklaut werden oder ob die eigenen Onlinekonten komplett geplündert werden, so hat sich die Arbeit schon gelohnt.

*(des@ct.de)* c't

***Download Sicherheits-Checklisten:***
***ct.de/yzc8***