BUZZWORD

Endlich! Endlich gibt es mal wieder eine Internetchallenge! Nachdem halbseidene Versuche wie die „Watermelondress-Challenge“ oder die umstrittene „Tide Pod Challenge“ uns nicht überzeugen konnten und die „Mannequin-Challenge“ und der „Harlem-Shake“ auch eher Trostpflaster waren, kommt jetzt nach der großen „Ice-Bucket-Challenge“ (lang, lang ist's her) der nächste Internet-hit: die #BottleCapChallenge. Marco Reus hat es schon getan. Justin Bieber auch. Ebenso Jason Statham und Ellie Goulding.

Aber was genau denn nun? Die Älteren unter uns werden sich noch an den berühmten Roundhouse-Kick von Chuck Norris erinnern, bei dem er sich einmal um die eigene Achse dreht und seinen Gegner mit einem dynamischen Fußtritt um zwei oder drei Zähne erleichtert. Im Gegensatz zur Chuck-Norris-Variante geht es bei der #BottleCapChallenge aber nicht darum, seinem Gegenüber den Kiefer oder die Rippen zu brechen. Stattdessen soll mit dem Schwung des Tritts der Schraubverschluss einer Flasche geöffnet werden. Wo genau der Ursprung dieser sportlich herausfordernden Challenge liegt, ist wie so oft nicht klar. Es wird gemutmaßt, dass der Taekwondo-Profi Farabi Davletchin ihn als #FaraKicksChallenge etablieren wollte und unter anderem Jackie Chan nominierte, ebenfalls ein solches Video zu posten. Irgendwie verselbstständigte sich dann das Ganze und wurde unter dem Namen #BottleCapChallenge, zu Deutsch: Flaschenverschluss-Herausforderung, bekannt.

Wie immer gilt: Wer sich besonders viel Mühe gibt, bekommt auch besonders viel Applaus. So kickt Marco Reus den Deckel von der Babyflasche seiner jüngst geborenen Tochter gekonnt herunter. Irritierenderweise mit Schnuller im Mund. Model Kendall Jenner öffnet eine Flasche zwar ohne Kick, dafür elegant mit den Füßen vom Jetski aus. Mariah Carey wiederum wird bereits als inoffizielle Gewinnerin der Challenge gefeiert, da sie den Verschluss nur mithilfe ihrer höchsten Töne wegkatapultiert. *Vanessa Casper*

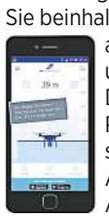
HACK & APP

Handy am Steuer: So passiert es nicht

Autofahrer dürfen ihr Handy am Steuer nicht in die Hand nehmen. Um schon die Versuchung zu minimieren, stellen sie es besser vor der Fahrt aus oder stumm, rät der TÜV Süd. Sinnvoll ist es auch, das Gerät an einem Platz zu verstauen, wo man es vom Steuer aus gar nicht erreichen kann. Das alles helfe, dem Reflex entgegenzuwirken, bei jeder Nachricht aufs Display zu blicken. Wer bei laufendem Motor ohne Freisprechanlage telefoniert oder das Handy aufnimmt, muss mit einem Bußgeld ab 100 Euro und einem Punkt in Flensburg rechnen. Verboten ist das laut ADAC auch bei Tablets oder Navigationsgeräten.

Wo darf die Drohne fliegen?

Auch wenn sie problemlos überall hinkommen: Drohnen dürfen längst nicht überall durch die Lüfte schwirren. Tatsächlich gibt es klare Regeln, die Piloten einhalten müssen. Wenn Sie sich unsicher sind, ob sie ihr Fluggerät an einem bestimmten Ort starten lassen dürfen, kann die DFS-Drohnen-App von der Deutschen Flugsicherung weiterhelfen. Sie beinhaltet interaktive Karten



aus amtlichen Quellen und zeigt für Standorte in Deutschland an, welche Regeln dort zu beachten sind. Die DFS-Drohnen-App gibt es kostenfrei für Android und iOS.

Spione suchen per Fake-Profil Kontakt

Soziale Medien bieten auch die Chance auf den nächsten Karriereschritt. Bei interessanten Anfragen klicken Nutzer daher schnell auf „bestätigen“ – und tappen leichtfertig in eine Falle

Von Raphael Satter

Katie Jones war in Washington gut vernetzt. Ihre Kontakte reichten bis in die höchsten politischen Kreise. Kein Wunder: Laut ihrem Linkedin-Profil hatte sie einen Job in einem renommierten Institut. Ganz nebenbei wirkte die rotblonde Frau in den Dreißigern auch optisch äußerst attraktiv. Was aber zumindest auf Anhieb nicht zu erkennen war: Diese Frau hat nie existiert. Es handelte sich vielmehr um einen von unzähligen Fake-Accounts auf der Onlineplattform. Das Foto von Jones wurde Experten zufolge vermutlich mithilfe von künstlicher Intelligenz erstellt. „Ich bin überzeugt, dass dies ein fingiertes Gesicht ist“, sagt Mario Klingemann, der seit Jahren mit künstlich generierten Porträts experimentiert und nach eigenen Angaben Zehntausende derartige Bilder überprüft hat. Der kalifornische Experte Hao Li verweist auf Ungereimtheiten im Bereich der Augen, den unnatürlichen Glanz der Haare und verschmierte Flächen auf der linken Wange.

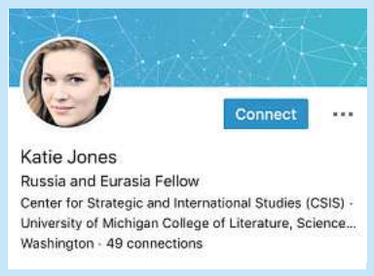
Auch die Vorgehensweise folgt einem Muster, das in den sozialen Medien immer öfter in Erscheinung tritt. „Das riecht sehr nach einer von einem Staat organisierten Operation“, sagt Jonas Parello-Plesner, der für die in Dänemark ansässige Stiftung Alliance of Democracies arbeitet und vor einigen Jahren selbst zum Ziel einer über Linkedin gestarteten Spionageaktion wurde.

Nicht nur ein Stellenmarkt, auch Fundgrube für Spione

William Evanina, der das National Counterintelligence and Security Center der USA leitet, wirft vor allem China vor, mit Fake-Profilen auf Linkedin amerikanische Zielpersonen ins Visier zu nehmen – und zwar in „massivem Umfang“. „Anstatt einen Spion in irgendein Parkhaus in den USA zu entsenden, um jemanden zu rekrutieren, ist es viel effizienter, hinter einem Computer in Shanghai zu sitzen und Freundschaftsanfragen an 30 000 Personen zu schicken“, erklärte er auf Anfrage der Nachrichtenagentur Associated Press (AP) in einer schriftlichen Stellungnahme.

Im Mai wurde der pensionierte CIA-Agent Kevin Mallory zu 20 Jahren Haft verurteilt, weil er Informationen über Geheimoperationen an Peking weitergereicht haben soll. Ausgangspunkt der Verbindungen des Mannes nach China war offenbar eine Linkedin-Anfrage eines gegnerischen Spions, der sich zunächst als Personalvermittler ausgegeben hatte.

Anders als bei Facebook, wo der Fokus auf Freunden und Verwandten liegt, geht es bei Linkedin für die meisten Nutzer um die Pflege und den Aufbau eines beruflichen Netzwerks. Insofern ist es nicht unüblich, Lebensläufe oder Projektideen mit Fremden zu teilen und allein auf Grundlage der in den Profilen angegebenen Informationen Kontakte zu knüpfen. Das hat die Plattform nicht nur zu einem riesigen Stellenmarkt gemacht, sondern eben auch zu einer Fundgrube für Spione.



Die Associated Press (AP) hat herausgefunden, dass es sich bei „Katie Jones“ um eines von vielen Phantomprofilen handelt, die auf der Social-Media-Plattform Linkedin lauern. FOTO: AP

Linkedin geht routinemäßig gegen Fake-Profile vor

Die Entwicklung bereitet westlichen Geheimdiensten Sorgen. In Großbritannien, Frankreich und Deutschland haben die zuständigen Institutionen in den vergangenen Jahren bereits vor der Masche gewarnt.

Linkedin selbst erklärte auf Anfrage, dass routinemäßig gegen Fake-Profile vorgegangen werde. Allein in den ersten drei Monaten dieses Jahres seien Tausende derartige Accounts gelöscht worden. Nutzern werde empfohlen, „sich mit Leuten zu vernetzen, die man kennt und denen man vertraut – und nicht einfach mit allen“.

Das Katie-Jones-Profil hatte zwar lediglich 52 Kontakte – aber diese waren hochrangig genug, um für Glaubwürdigkeit zu sorgen. AP konnte mit etwa 40 Personen sprechen, die sich zwischen Anfang März und Anfang April mit der fiktiven Frau vernetzten. Viele von ihnen räumten ein, sie würden in der Regel alle Anfragen auf der Plattform ohne nähere Prüfung annehmen.

„Ich bin wahrscheinlich der schlechteste Linkedin-Nutzer in der Geschichte von Linkedin“, sagte der Wirtschaftsexperte Paul Winfree, der im ersten Jahr der Präsidentschaft von Donald Trump im Weißen Haus tätig war und im Mai als Kandidat für einen wichtigen Posten in der US-Notenbank Fed gehandelt wurde. Er logge sich nur selten auf der Seite ein – und wenn, dann klicke er meist bei allen aufgestauten Anfragen auf bestätigen. Am 28. März tat er dies auch im Falle von Jones.

Lionel Fatton, der an der Webster University in Genf Ostasienwissenschaften lehrt, zögerte laut eigenen Angaben einen kurzen Moment, weil er einer Frau mit dem Namen nie begegnet war. „Ich kann mich erinnern, dass ich gestutzt habe“, sagte er AP. Aber dann habe er gedacht: „Was schadet es?“

Das Jones-Profil ist inzwischen verschwunden

Der Experte Parello-Plesner betont, dass der potenzielle Schaden auf subtile Art erfolge. Die Vernetzung mit einem Profil wie dem von Jones ermögliche dessen Urhebern anschließend eine direkte Kontaktaufnahme, sagt er. Zugleich könnten andere Nutzer die Verknüpfung als eine Art Empfehlung werten. „Man ist weniger wachsam und verleitet andere dazu, ihrerseits weniger wachsam zu sein.“

Auch Keir Giles, ein Russland-Experte vom Londoner Institut Chatham House, erhielt eine Anfrage von Jones. Da er kürzlich mit einem davon unabhängigen Spionagefall zu tun gehabt hatte, bei dem Kritiker des russischen Software-Unternehmens Kaspersky Lab ins Visier genommen wurden, machte ihn die Anfrage misstrauisch. Laut Profil arbeitete die Frau seit Jahren als Russland- und Eurasienexpertin am Center for Strategic and International Studies (CSIS) in Washington. Und Giles sagte sich: Wenn das stimmen würde, „dann müsste ich von ihr gehört haben“.

Der CSIS-Sprecher Andrew Schwartz bestätigte gegenüber AP, dass „niemand mit dem Namen Katie Jones“ für das Institut arbeite. Im Jones-Profil war auch ein Abschluss von der University of Michigan erwähnt. Doch die Hochschule erklärte auf Anfrage, sie wisse nichts von einer Person mit diesem Namen, die einen entsprechenden Abschluss gemacht habe. Kurz nachdem AP das Unternehmen Linkedin um eine Stellungnahme gebeten hatte, verschwand das Jones-Profil. Direkt an Jones gerichtete Nachrichten – über die Onlineplattform sowie über eine im Profil genannte E-Mail-Adresse – waren zuvor unbeantwortet geblieben.

Gefälschte Profile auf Facebook

Nicht nur beim Karriereportal Linkedin tummeln sich zahlreiche Fake-Accounts. Auch für andere soziale Netzwerke sind sie ein Problem. In welchem Ausmaß, das zeigen Zahlen, die das US-Netzwerk Facebook Ende Mai veröffentlichte. Demnach hat Facebook allein im ersten Quartal dieses Jahres rund 2,2 Milliarden gefälschte Accounts gelöscht. Ein großer Teil davon werde von Spammern angelegt, die die Plattform für dubiose Werbung nutzen wollen, wie der zuständige Facebook-Manager Guy Rosen erläuterte. Sie versuchten, automatisiert jeweils Hunderttausende oder sogar Millionen Fake-Konten zu erzeugen. Facebook machte keine Angaben dazu, in welchem Maße die gefälschten Profile nach Erkenntnissen des Onlinenetzwerks auch für politische Einflussnahme angelegt werden. Die Zahl der von Facebook gelöschten Fake-Konten steigt allerdings kontinuierlich an.

RND-ILLUSTRATION: PATAN

Smartphones „grenzsicher“ machen

Meine Daten bekommt ihr nicht: Wie schützt man seine Geräte vor übergriffigen Staaten?

Von Dirk Averesch

Es kommt nicht häufig vor, aber immer wieder hört man von Reisenden, die am Flughafen oder an der Grenze aufgefordert werden, ihr Smartphone zu entsperren und auszuhändigen. Laut einer Recherche unter anderem der „Süddeutschen Zeitung“ installiert die chinesische Regierung Touristen bei der Einreise eine Überwachungs-App auf deren Smartphones, um sie dadurch auszuspähen.

Ob und wie man sich auf so eine Situation vorbereiten möchte, hängt ganz von der eigenen Risikoeinschätzung ab, erklärt die Bürgerrechtsorganisation Electronic Frontier Foundation (EFF). Faktoren, die in die persönliche Bewertung einfließen können, seien unter anderem die eigene Reisegeschichte, also Länder, in die man schon eingereist ist. Oder die Schutzwürdigkeit der Daten, die man besitzt oder mit denen man arbeitet. Zu diesen Maßnahmen rät die EFF:

Ausspähversuchen lässt sich einiges entgegensetzen. FOTO: ANATOLIY SIZOV/GETTY

- **Back-up anlegen:** Egal, ob Smartphone, Tablet oder Notebook – vor der Reise sollten alle Daten auf Geräten, die man mitnimmt, gesichert werden. So schützt man sich vor einem Totalverlust, wenn Geräte beschlagnahmt werden.
- **Reisesmartphone anschaffen:** Man kann sich überlegen, ein Gerät mit weniger oder gar keinen sensiblen Daten nur vorübergehend zu nutzen – also etwa für die Dauer einer Reise.
- **Daten löschen oder auslagern:** Wer mit seinem regulären Gerät reist, sollte möglichst viele Daten darauf löschen – von Mails über den Browserverlauf bis hin zu Dokumenten. Alternativ kann man möglichst viele Daten in einen Onlinespeicher auslagern – am besten verschlüsselt.
- **Datenverstecke nützen nichts:** Es gibt Apps, die Dokumente oder Bilder verbergen können. Ebenso lassen sich versteckte Partitionen auf Notebook-Festplatten einrichten. Allein: Grenzbeamte wissen das meist auch und suchen danach.
- **Keine biometrischen Zugangssperren nutzen:** Fingerabdruck-, Iris-, Venen- oder Gesichtsscanner sind zum Freigeben von Geräten praktisch, aber längst nicht so sicher wie starke Passwörter.
- **Verschlüsseln:** Die EFF rät dazu, das Smartphone und die komplette Notebook-Festplatte zu verschlüsseln. Bei iPhones läuft das automatisch übers Passwort. Bei Androiden muss man dies in den Einstellungen aktivieren. Mac-Books verschlüsselt man mit dem integrierten Filevault, Windows-Notebooks mit Bitlocker oder dem freien Veracrypt.
- **Ausschalten:** Bevor man an die Grenze gelangt oder kontrolliert wird, sollte man seine Geräte ausschalten. So kann man eventuell Angriffe verhindern.
- **Keine unüblichen Vorsichtsmaßnahmen:** Diese könnten Grenzbeamte misstrauisch werden lassen, warnt die EFF. Wer etwa ein neues oder sichtlich ungenutztes Telefon aus der Tasche zieht, sein reguläres Gerät aber versteckt hält und dabei auffällt, riskiert erst recht, eingehend untersucht zu werden.
- **Nach einer Kontrolle:** Wer den Eindruck hat, dass trotz der Vorsichtsmaßnahmen Zugangsdaten zu Geräten oder Diensten ausspioniert worden sind, sollte die Passwörter ändern. Beim Verdacht, dass Spionagesoftware installiert wurde, sollte man Mobilgeräte auf die Werkseinstellungen zurücksetzen oder sein Notebook neu aufsetzen.