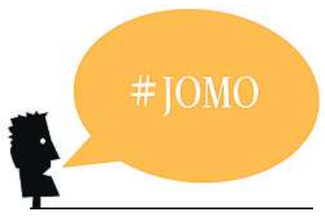
BUZZWORD



Greta Thunberg fährt mit der Deutschen Bahn und muss auf dem Boden sitzen. Das entsprechende Foto dazu postet die Klimaaktivistin unter anderem auf Twitter. Wenn 16-jährige Mädchen in sozialen Medien Fotos posten, ist das kein Ereignis. Wenn Greta Thunberg ein Foto von sich in einem überfüllten ICE postet, schon.

Es dauert nicht lange, da werden Greta-Follower und Follower von Gretas Gefolgschaft auf den Beitrag der Klimaaktivistin aufmerksam. Die Netzgemeinde ist gespalten in jene, die auf den Greta- und jene, die auf den Bahnbashing-zug aufspringen. Geht auch beides?

Es dauert nicht lange, da reagiert die Bahn und befeuert die Diskussion auf ihre eigene Art mit einem Spagat aus Imagepflege und beleidigter Leberwurst. Das sieht in etwa so aus: „Nett, dass Sie sich für eine Reise mit der Deutschen Bahn entschieden haben. In Zukunft bemühen wir uns noch mehr, Ihnen das anzubieten, was wir Ihnen versprechen. Noch netter wäre es, wenn Sie unser Bemühen schon jetzt würdigten, auch wenn Sie nicht zu hundert Prozent in den Genuss unseres Services gekommen sind.“ Das Netz tobt: noch mehr Bahnbashing von den einen, noch mehr Gretabashing von den anderen.

Es dauert nicht lange und die Medien reagieren auf das Spektakel. Bald darauf schalten sich Politiker jeglicher Couleur in die Debatte ein. Die einen üben sich in Gretabashing, die anderen in ... Sie wissen schon.

In der Zwischenzeit ist Greta übrigens in ihrer schwedischen Heimat angekommen. Ob sie den Rest ihrer Reise auf dem Boden sitzend oder nach ihrer Sitzplatzreservierung suchend verbracht hat, weiß man nicht genau – es gibt keinen entsprechenden Post der Aktivistin.

JOMO, unser aktuelles Buzzword, steht übrigens für „joy of missing out“ und beschreibt die Freude, etwas in den sozialen Netzwerken zu verpassen. Man kann sich nur wünschen, dass diese Freude in Zukunft mehr Menschen überkommt.

Patrick Fam

HACK & APP

Live-Fotos als GIFs auf Twitter

Auf Twitter lassen sich nun auch die Live-Fotos genannten Ultrakurzvideos von iPhones einbinden. Wird eines der drei Sekunden kurzen Filmchen zum Posten ausgewählt, wandelt Twitter es auf Wunsch in eine GIF-Animation um. Alternativ ist weiterhin das Veröffentlichen eines Einzelbildes möglich, so wie es auf Twitter bislang üblich war, wenn aus einem Live-Foto ein Tweet werden sollte. Die Tonspur, die ein Live-Foto auf dem Gerät noch hat, wird allerdings nicht übertragen. Bei der Funktion nimmt die Kamera die 1,5 Sekunden vor und nach dem Foto auf.

Notiz-Apps: Fixe Ideen fix festhalten

Einkaufslisten, Telefonnummern oder die Erinnerung ans Staubsaugen: digital festgehaltene Notizen sind praktisch. Wem dabei die Nutzung auf mehreren Endgeräten wichtig ist, für den sind bei Windows-PCs Google Notizen und Sticky Notes empfehlenswert. Bei Apple-Geräten bietet sich die App Notizen an. Für etwas höhere Ansprüche sind insbesondere Evernote und Microsoft OneNote geeignet. Bei Evernote wird bei zusätzlichen Funktionen eine Abo-Gebühr fällig, für die meisten Aufgaben ist die Basisversion aber ausreichend.

Hilfe, ich wurde gehackt! Und jetzt?

Viele Unternehmen sind schon einmal Opfer von Cyberattacken geworden. Was jedoch oft untergeht: Die meisten Angriffe aus dem Netz richten sich gegen ganz gewöhnliche Internetnutzer

Von Alena Hecker


RND-ILLUSTRATION

Oft sind es nur die spektakulären Fälle, über die berichtet wird: Hacker, die etwa in die Netzwerke des Autokonzerns BMW eindringen oder die Europäische Zentralbank (EZB) im September dazu zwangen, eine ihrer Webseiten vom Netz zu nehmen.

Was bei solchen Geschichten aber häufig untergeht: Hackerangriffe zielen längst nicht nur auf große Unternehmen ab. Einer Studie des Digitalverbandes Bitkom zufolge ist 2018 jeder zweite Internetnutzer in Deutschland Opfer von Cyberkriminalität geworden. Bei fast einem Viertel der Befragten ging es um persönliche Daten, die illegal genutzt oder weitergegeben wurden – Passwörter, Kreditkarteninformationen, gestohlene Identitäten.

Wie erkennt man einen Hackerangriff?

Manchmal sind es Beschwerden von Freunden und Bekannten, die stutzig machen: Warum man plötzlich so unsinnige Nachrichten verschicke oder leere Mails mit Anhang? Offensichtlicher ist es, wenn die Bank sich meldet und auf verdächtige Kreditkartenzahlungen oder Abbuchungen aufmerksam macht. Auch große Plattformen wie Facebook und Google benachrichtigen ihre Nutzer, wenn sie Auffälligkeiten bemerken – etwa ein unbekanntes Gerät, das aufs Konto zugreift. Genauso kann es ein Indiz sein, dass sich der Internetbrowser ganz kurz öffnet und wieder schließt oder Programme ungewöhnlich schnell abstürzen.

Mit dem Identity Leak Checker hat das Hasso-Plattner-Institut ein Werkzeug entwickelt, mit dem sich überprüfen lässt, ob das Passwort eines E-Mail-Accounts ausgespäht wurde. Dafür reicht es, auf der Website die eigene E-Mail-Adresse einzugeben. Das Ergebnis geht wenige Sekunden später an die angegebene E-Mail-Adresse, bietet jedoch nur teilweise Klarheit: Denn selbst wenn eine E-Mail-Adresse nicht in der Datenbank auftaucht, kann es trotzdem sein, dass an anderer Stelle persönliche Daten gestohlen wurden.

Was kann ich tun, wenn ich gehackt wurde?

Wer den Verdacht hat, der Computer oder das Smartphone könne gehackt worden sein, sollte zuallererst Ruhe bewahren. „Wenn du im Panikmodus bist, wirst du womöglich nicht die richtige Entscheidung treffen“, erklärt Claudio Guarnieri im Gespräch mit dem Magazin vice.com. Er ist selbst Hacker und arbeitet als Sicherheitsforscher für Amnesty International. Seine Empfehlung: Betroffene sollten die Internetverbindung sofort kappen, noch besser aber das gesamte Gerät ausschalten. „Entweder um zu verhindern, dass Daten verloren gehen oder gestohlen werden, oder um der Selbstlöschung der Malware zuvorzukommen. Sie könnte als Beweis in einem späteren Verfahren dienen.“

> Im Panikmodus wirst du womöglich nicht die richtige Entscheidung treffen.

Da Hacker häufig über abgefangene Passwörter Zugriff auf Konten und Geräte bekommen, sollten im Anschluss sämtliche Passwörter von Diensten erneuert werden, die auf dem betroffenen Gerät verwendet wurden. Ein sicheres Passwort beinhaltet mindestens zwölf Zeichen, darunter Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen.

Oft ist es ratsam, eine Person hinzuziehen, die sich auskennt und bei weiteren Schritten helfen kann. Und schließlich sollte der Vorfall auch bei der Polizei gemeldet werden. Das geht zum Beispiel unkompliziert in den Internetwachen der einzelnen Bundesländer.

Kann ich mich gegen Hackerangriffe absichern?

Spezielle Versicherungsangebote mit Namen wie Internet-Rechtsschutz, Cyber-Versicherung oder auch Internetschutz versprechen Hilfe bei Betrug im Onlineshopping, bei Identitätsmissbrauch und Cybermobbing. Ein Angebot, das etwa in Fällen von Cybermobbing hilfreich sein könnte: „Die kompetente Organisation und Finanzierung von technischen Experten zur Löschung von diskreditierenden Daten wäre prima“, so Peter Grieble von der Verbraucherzentrale in Baden-Württemberg. Problematisch findet er jedoch die geltenden Konditionen der Anbieter: „Einige Versicherer beschränken die Anzahl der Löschversuche auf drei oder es werden anfallende Kosten nur bis zu einer Höhe von einigen Hundert Euro übernommen. Dadurch ist der Wert der Hilfe begrenzt.“

Wie kann ich vorbeugen?

- **Software aktuell halten:** Updates enthalten Softwareanpassungen, die den nächsten Angriff verhindern können.
- **Skeptisch sein:** Besondere Vorsicht ist geboten, wenn ein Programm oder eine Nachricht zu einem Klick oder einem Download auffordert.
- **Passwortmanager mit Zwei-Faktor-Authentifizierung nutzen:** Diese Programme erzeugen und speichern Passwörter in einer verschlüsselten Datei auf PCs, Notebooks und Smartphones. Nutzer müssen sich dann nur noch ein einziges Passwort merken – das Masterpasswort. Manager mit Zwei-Faktor-Authentifizierung verlangen bei der Anmeldung neben dem Masterpasswort zusätzlich einen zweiten Schlüssel, etwa einen Fingerabdruck.
- **Apps überprüfen:** Dass eine vermeintlich harmlose App viel Schaden anrichten könnte, zeigt sich zum Beispiel bei ihrer Anfrage auf Zugriffsrechte, die gar nichts mit ihrer eigentlichen Funktion zu tun haben: eine Kalender-App, die auf Kamera, Mikro, Galerie, das Adressbuch und Geodaten zugreifen möchte? Sofort deinstallieren!
- **Daten sichern:** Auch ohne Hackerangriff können Daten verschwinden. Deshalb sollte man sie an zwei anderen Orten als auf dem PC speichern.

Ein Passwort reicht nicht mehr: Viele Onlinedienste setzen zusätzlich zum Passwort noch auf einen zweiten Sicherheitsfaktor – so zum Beispiel auch Twitter.

FOTO: ANDREA WARNECKE/DPA

IM TEST

Was kann Googles neues Mesh-Wifi?

Netzabdeckung für große Flächen und einfache Installation: Im Test überzeugt Googles Nest Wifi – mit kleineren Abstrichen

Von Carolin Burchardt

Der erste Eindruck ist positiv: Optisch beeindruckt Googles neues Nest Wifi auf Anhieb – und kann sich durchaus mit den edlen Designs anderer Hersteller messen lassen. Zwei dezente und fein abgerundete weiße Geräte entnehmen wir dem Karton, den Router samt Repeater. Beide machen auch in der Hand einen wertigen Eindruck.

Zusammen bilden sie Googles neues Mesh-System, also zwei Funkstationen, die unsere Wohnung mit schnellerem W-LAN versorgen sollen als die bisherige „Bambusleitung“, die immer wieder für familieninternen Frust sorgt. Was also kann Google?

Die Installation erfolgt per Smarthome-App. Fix den Router an unser Heimnetzwerk angeschlossen und schon taucht das neue Gerät auf: „Nest-Wifi-Router wurde gefunden – Möchtest du dieses Gerät einrichten?“, fragt die App. Der weitere Prozess verläuft flüssig, QR-Code unter dem Gerät gescannt und schon wird das neue Heimnetzwerk, dem wir noch einen lustigen Namen verpassen, erstellt. Der gesamte Vorgang nimmt nur wenige Minuten in Anspruch und ist kinderleicht. Ein erster Upload- und Downloadgeschwindigkeitstest zeigt: Das Nest Wifi läuft tatsächlich schneller, als es unser bisheriges Netzwerk tat – zufriedene Gesichter überall. Google selbst bewertet die aktuelle Geschwindigkeit in der App mit „Gut“. Das suggeriert: Offenbar ist da noch Luft nach oben.


Das Google Wifi Nest im Set kostet 259 Euro – darin enthalten sind der Router und ein Zugangspunkt.

FOTO: GOOGLE

Etwas hakeliger gerät die Einrichtung des Zugangspunktes. Wir platzieren das Gerät, das auch wunderbar als Smart-Speaker fungiert, dafür im Kinderzimmer, verbunden mit der Hoffnung auf eine stabile Zockerleitung. Diese war dem Junior bisher im äußersten Winkel der 140 Quadratmeter großen Wohnung trotz Repeater versagt geblieben. Doch Googles Mesh-System verspricht auch derart große Flächen mit einem stabilen Netz abzudecken. Leider weicht die Hoffnung schneller Ernüchterung. Die Smart Home App kann den Zugangspunkt nicht finden. Also schneller Anruf beim Google-Technik-Support mit der Erkenntnis: Der Fehler liegt bei uns. Zum Einrichten ist es erforderlich, dass beide Geräte direkt nebeneinander stehen und nicht am jeweiligen Bestimmungsort – in unserem Fall trennten sie etwa 20 Meter und zwei Leichtbauwände voneinander. Ein Installationshinweis dazu von Google wäre nett gewesen, doch den suchten wir vergebens.

Nun gelingt auch die Einrichtung des Zugangspunktes fix, und tatsächlich ist die Wohnung mit (halbwegs) stabilem W-LAN versorgt. Dem Junior reicht die Geschwindigkeit zwar nicht zum Zocken, doch eine Whatsapp-Nachricht ist nun auch im äußersten Winkel der Wohnung schnell verschickt. Unser Fazit: Eine deutliche Verbesserung der Netzabdeckung, aber noch nicht die finale Lösung für unsere Wohnsituation.