AUFBRUCH
Datensicherheit

Wie wir im Internet geschützt bleiben

Einblick

Im Gespräch mit zwei Sicherheits-ingenieuren von Google

Einstellung

Praktische Tipps, wie Sie ihre Online-Accounts schützen können

Ernstfall

Wo Experten die Abwehr von Cyberangriffen üben

Google

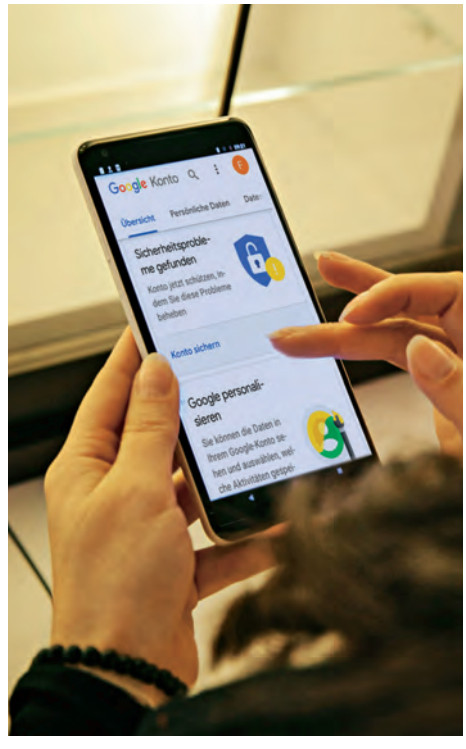
EINFÜHRUNG

Liebe Leserin, lieber Leser,

der Wert von Sicherheit wird besonders dann klar, wenn wir ihr Gegenteil erfahren: die Unsicherheit. Das gilt auch in der digitalen Welt. Wer seinen Computer mit einem Virus infizierte, weil er einen unbekannten Mailanhang öffnete, weiß, wovon die Rede ist. Andere haben erfahren, wie ihr Account gehackt wurde und Spam-Mails an alle Kontakte gingen — ein ähnlich großes Ärgernis.

Auf der ganzen Welt arbeiten Experten daran, dass Ihre Daten sicher sind. So auch die Ingenieure von Google, die sich um die Sicherheit der Google-Dienste kümmern. In diesem Heft zeigen wir Ihnen, wie wir arbeiten und vermitteln Tipps für einen besseren Schutz im Internet.

Ihr Team von Google



Das Google-Konto ist der Ort, an dem jeder angemeldete Nutzer zentrale Datenschutz- und Sicherheitseinstellungen vornehmen kann. Mehr Informationen dazu auf myaccount.google.com

IMPRESSUM

Dienstanbieterin: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland
Tel: +353 1 543 1000 | Fax: +353 1 436 1001 | E-Mail: support-de@google.com
Vertreten durch die Geschäftsführerinnen: Fionnuala Meehan, Elizabeth M. Cunningham
Google Ireland Limited ist eine nach irischem Recht gegründete und registrierte Gesellschaft. Registernummer: 368047.
Umsatzsteuer-ID.-Nr.: IE6388047V

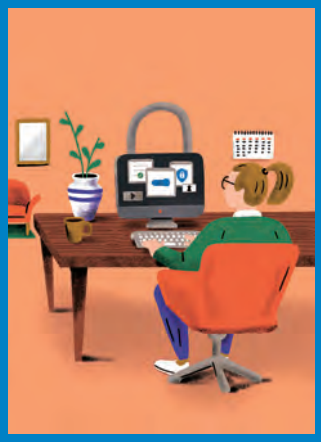
Dies ist eine Anzeigensonderveröffentlichung von Google. Danke an das Team von SZ Scala GmbH.

INHALT

Welche Daten hinterlasse ich im Netz?

Die digitalen Weltverbesserer: S. 14

Googles Beitrag zur Sicherheit der Nutzer



Der Schlüssel zum Schutz: S. 12

Drei wichtige Anlaufstellen für ein sicheres Internet

Der Mann, der die Nutzer besser verstehen will: S. 22

Googles Zukunfts-werkstatt
Seite 17

Titelfoto: Mike Kemp | Foto linke Seite: Felix Brüggemann; Fotos rechte Seite: Reto Sterchi, Felix Brüggemann | Illustration: Robert Samuel Hanson

Ich hätte da mal ein paar Fragen

Wie ist das mit
unseren Daten im Internet:
Wo entstehen sie, wer hat Zugriff, und
wie können wir sie am besten schützen?
Experten geben Antworten

Welche Spuren hinterlasse ich eigentlich im Netz?

Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI): »Zunächst einmal sind dies die Daten, die jeder Internetnutzer freiwillig von sich preisgibt, beispielsweise auf seiner eigenen Webseite oder in sozialen Netzwerken. Darüber hinaus gibt es Daten, von denen viele Nutzerinnen und Nutzer gar nicht wissen, dass sie erhoben werden. Dazu gehören zum Beispiel die IP-Adresse, die jedes Endgerät im Internet erhält, oder beim Onlineshopping Informationen über besuchte Webseiten, die Verweildauer auf einer Seite oder Links, die geklickt wurden.«

Kann ich verhindern, dass bestimmte Angaben übermittelt werden?

Michael Littger, Geschäftsführer des Vereins »Deutschland sicher im Netz«, DsiN: »Welche Daten ich eingebe, kann ich natürlich selbst bestimmen. Auf die technischen Daten, die entstehen, sobald ich mich im Internet bewege, habe ich nur bedingt Einfluss. Cookies kann ich ablehnen oder löschen. Auch meine IP-Adresse lässt sich mit entsprechenden Programmen relativ einfach verschleiern. Und wer nicht will, dass der smarte Lautsprecher, der im Wohnzimmer steht, indirekt mithört, weil er auf den Aktivierungsbefehl wartet, dem bleibt als Option immer noch: abschalten.«

Wer ist an meinen Daten überhaupt interessiert? Und weshalb?

Michael Littger, DsiN: »Für Unternehmen sind Nutzerdaten sehr wertvoll. Sie sammeln die Daten, die während der Verwendung ihrer Dienste entstehen, um ihre Produkte zu verbessern oder Werbung für Nutzer besser zuzuschneiden. Leider versuchen auch Internetkriminelle, an die Daten von Nutzern zu gelangen — zum Beispiel, um sie zu erpressen oder ihr Bankkonto zu plündern. Nicht vergessen sollte man die Möglichkeiten der Strafverfolgung durch Behörden wie die Polizei, die für ihre Ermittlungen zum Beispiel Navigationsdaten anfragen kann – natürlich nur nach richterlichem Beschluss.«

Wie können Kriminelle an meine Informationen gelangen?

Stephan Micklitz, globaler Entwicklungschef für Sicherheit und Datenschutz bei Google: »Die beiden häufigsten Wege, um illegal an Nutzerdaten zu gelangen, sind Phishing und Hacking. Beim Phishing spielt man dem Nutzer etwas vor, um ihn dazu zu bewegen, seine Daten freiwillig herauszugeben – zum Beispiel durch eine falsche Bank-Webseite, auf der der Nutzer gutgläubig seine Kontoinformationen eintippt. Beim Hacking bricht der Angreifer in ein Konto ein, zum Beispiel durch Schadprogramme. Meistens kombinieren Onlinekriminelle diese beiden Ansätze in irgendeiner Weise.«

Wie kann ich mich schützen?

Arne Schönbohm, BSI: »Sehr sinnvoll ist es, sich genau zu überlegen, welche Texte, Fotos oder Videos man ins Internet stellt. Fachleute sprechen dabei von ›Datensparsamkeit‹ und meinen zum Beispiel, dass man nur die Daten angeben sollte, die für eine digitale Dienstleistung zwingend notwendig sind. Um einem Datendiebstahl vorzubeugen, sind sichere Passwörter sowie die schnelle Installation neuer Updates essenziell. Wenn Nutzerinnen und Nutzer ferner ein Bewusstsein dafür entwickeln, dass es im Internet Betrüger gibt, die sie mit falschen Identitäten oder erfundenen Geschichten anschreiben, ist schon viel gewonnen.«

Protokolle: Serge Debrebant | Fotos: Jan von Holleben

Hilfe, mein Konto wurde gehackt! Was kann ich tun?

Michael Littger, DsiN: »Ich würde erst einmal den Anbieter kontaktieren und das Passwort wechseln. Bei kritischen Konten, etwa dem Bankkonto, kann auch eine vorläufige Sperrung sinnvoll sein. Um das Konto wiederherzustellen, ist es sinnvoll, eine alternative E-Mail-Adresse oder eine Mobilnummer zu hinterlassen, über die der Anbieter mich kontaktieren kann. Nach der Wiederherstellung würde ich mithilfe geeigneter Tools versuchen festzustellen, welcher Schaden entstanden ist – sowie zur Polizei gehen und Anzeige erstatten. Schließlich bin ich gerade Opfer eines Verbrechens geworden.«

Bin ich mit einem Smartphone leichter angreifbar als mit dem PC?

Mark Risher, Leiter des Produktmanagements für Internetsicherheit bei Google: »Smartphones sind von Haus aus gegen viele Gefahren geschützt, die früher bei PCs Probleme bereiteten. Bei der Entwicklung der Betriebssysteme für Smartphones haben Anbieter wie Google eine Menge Erfahrungen aus der Vergangenheit einfließen lassen. Allerdings rate ich Nutzern dringend, stets die Bildschirmsperre einzuschalten. Schließlich haben die meisten ihr Smartphone fast immer mit dabei, sodass es Dieben leicht fällt, es zu klauen.«

Wie kompliziert muss mein Passwort sein?

Michael Littger, DsiN: »Ein starkes Passwort sollte nicht in einem Wörterbuch zu finden sein, und neben Buchstaben auch Zahlen und Sonderzeichen enthalten. In unseren Schulungen bringen wir den Teilnehmern einfache Tricks bei, um starke Passwörter zu entwickeln, die man sich gut merken kann. Hier die Merksatzregel: Ich überlege mir einen Satz wie ›Mein Kumpel Walter wurde 1996 geboren!‹ Dann reihe ich die Anfangsbuchstaben und Zahlen aneinander: MKWw1996g! Eine andere Methode ist die Drei-Wort-Regel. Ich überlege mir drei Wörter über ein Ereignis, das ich mir dann ebenfalls merken muss. ›FrauKarneval1994‹. Das könnte sich darauf beziehen, dass jemand seine Frau beim Karneval 1994 kennengelernt hat.«

Brauche ich einen Virenscanner?

Arne Schönbohm, BSI: »Eine gute Antiviren-Software ist ein Muss, sobald man mit PCs online unterwegs ist. Untersuchungen des BSI haben gezeigt, dass ein ungeschützter PC, mit dem man im Internet surft, innerhalb weniger Minuten mit Schadsoftware infiziert ist. Wichtig ist, die Software regelmäßig zu aktualisieren, weil täglich neue Varianten von Schädlingen auftreten. Mobile Geräte wie Smartphones sind auch ohne Antiviren-Software sicher. Hier empfehle ich Nutzern vor allem, ihre Apps in seriösen Stores herunterzuladen.«

Wie sinnvoll ist ein Passwort-Manager?

Tadek Pietraszek, Chefentwickler für Kontosicherheit bei Google: »Viele Nutzer verwenden das gleiche Passwort auf mehreren Webseiten, weil sie sich nicht viele Passwörter auf einmal merken wollen. Wenn Angreifer dieses Passwort aber herausfinden, sind sofort mehrere Webseiten gleichzeitig gefährdet. Deswegen raten wir, Passwörter niemals wiederzuverwenden. Außerdem passiert es immer wieder, dass Nutzer ein Passwort versehentlich auf einer Webseite eintippen, die von Betrügern gebaut wurde — gerade dann, wenn sie es oft benutzen. Mit einem Passwort-Manager können Nutzer beide Probleme auf einmal lösen. Sie müssen sich ihre Passwörter nicht mehr merken und damit entfällt auch die Motivation, Passwörter wiederzuverwenden. Außerdem benutzt der Passwort-Manager ein Passwort nur auf der richtigen Webseite; im Gegensatz zu Menschen fällt er nicht auf Webseiten von Betrügern herein. Wichtig ist aber, nur Passwort-Manager seriöser Anbieter zu verwenden – zum Beispiel Dashlane, der Keeper Passwort-Manager oder der integrierte Passwort-Manager von Googles Internet-Browser Chrome.«

Wie soll ich auf Meldungen von gehackten Accounts reagieren, wie sie erst kürzlich zu lesen waren?

Michael Littger, DsiN: »Vielen fällt es schwer, Meldungen über einen Supervirus oder über Millionen gehackter Konten einzuordnen. Wir nennen diese Fähigkeit die ›Risikoeinschätzungskompetenz‹. Das kann einerseits dazu führen, dass man eine Gefahr überschätzt und sich grundlos Sorgen macht. Andererseits kann es dazu führen, dass man eine Gefahr unterschätzt. Unsere App ›Sicherheitsbarometer‹ informiert zu aktuellen Gefahren mit konkreten Hinweisen zum Schutz.«

Welche Entwicklungen sollte ich im Auge behalten?

Arne Schönbohm, BSI: »Nicht nur Computer und Mobilgeräte, auch Fernseher, Heizungen und Sicherheitskameras können heute vernetzt sein. Man spricht auch vom Smart Home, von intelligenten, internetfähigen Geräten für zu Hause. Hier sollten Verbraucherinnen und Verbraucher besonders auf ihre Sicherheit achten. Dazu gehört, die Software regelmäßig upzudaten und den Router mit sicheren Passwörtern zu schützen. Auch beim Kauf eines Gerätes sollte die IT-Sicherheit erwogen werden. Um hier eine Entscheidungshilfe zu bieten, plant das BSI die Einführung eines IT-Sicherheitskennzeichens.

Welche Rolle spielen Staat und Politik bei der Datensicherheit?

Michael Littger, DsiN: »Der Staat kann die Digitalkompetenz in der Bevölkerung und bei Unternehmen mit der gezielten Unterstützung von Aufklärungsangeboten verbessern. Außerdem hält er technische Expertise zu aktuellen Bedrohungslagen vor – diese leistet zum Beispiel das BSI. Staat und Politik spielen darüber hinaus eine wichtige Rolle in der Regulierung und Gesetzgebung. Hier ist vor allem die Datenschutzgrundverordnung zu nennen, die 2018 in Kraft getreten ist und unter anderem auch regelt, wie Unternehmen Nutzerdaten schützen müssen.«

Fraunhofer-Institut für Sichere Informationstechnologie (SIT)

WER STECKT DAHINTER?

Das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) gehört zur Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V., die sich vor allem auf anwendungsbezogene Wissenschaft konzentriert. Das Fraunhofer SIT forscht im Bereich Cybersicherheit, hat seinen Sitz in Darmstadt, Birlinghoven und Mittweida und beschäftigt rund 180 Mitarbeiter.

WAS MACHT DIE ORGANISATION?

Das Fraunhofer-Institut für SIT entwickelt IT-Sicherheitskonzepte und sichere Software-Lösungen für Unternehmen und Behörden und überprüft die Sicherheit von Drittanbieter-Produkten. Im »Lernlabor Cybersicherheit« können sich Fach- und Führungskräfte aus Wirtschaft und Verwaltung weiterbilden.

WO KANN ICH MEHR ERFAHREN?

Institut: **sit.fraunhofer.de**

Lernlabor Cybersecurity:
academy.fraunhofer.de/de/weiterbildung/information-kommunikation/cybersicherheit.html

Fraunhofer SIT

Beim Thema Onlinesicherheit fühlen sich viele Nutzerinnen und Nutzer überfordert. Dabei kann es schon helfen, sich an **ein paar einfache Regeln** zu halten. Mark Risher und Stephan Micklitz von Google klären auf

Auf dem Dach der Münchner Google-Niederlassung: Die Datensicherheitsingenieure Mark Risher (links) und Stephan Micklitz.

» Am liebsten würden wir Passwörter ganz abschaffen «

Herr Risher, Sie leiten bei Google das Produktmanagement im Bereich Internetsicherheit. Sind Sie auch schon einmal auf eine Betrugsattacke im Internet hereingefallen?

Mark Risher: Mir fällt jetzt kein konkretes Beispiel ein, aber ich gehe schwer davon aus. Wie alle mache ich Fehler, wenn ich mich im Netz bewege. Vor Kurzem habe ich zum Beispiel bei der falschen Webseite mein Google-Passwort eingetippt. Zum Glück hatte ich die Chrome-Erweiterung »Passwort-Warnung« installiert, die mich auf mein Versehen hingewiesen hat. Natürlich habe ich mein Passwort dann sofort geändert.

Stephan Micklitz, Entwicklungschef für Sicherheit und Datenschutz: Das ist nur menschlich. Sobald wir Nutzer uns ein Passwort gemerkt haben, kann es schnell passieren, dass wir es achtlos eintippen, ohne darauf zu achten, wo genau wir es eingeben.

Risher: Am liebsten würden wir den Gebrauch von Passwörtern abschaffen, aber leider geht das nicht so einfach.

Was ist denn an Passwörtern so schlimm?

Risher: Sie haben viele Nachteile: Man kann sie leicht klauen, man kann sie sich aber nur schwer merken. Passwörter sind umständlich in der Handhabung. Viele Nutzerinnen und Nutzer glauben, dass ein Passwort möglichst lang und kompliziert sein sollte – obwohl das sogar das Sicherheitsrisiko vergrößert. Komplizierte Passwörter verführen sogar dazu, sie mehrmals zu verwenden, wodurch sich Nutzer erst recht gefährden.

Micklitz: Je seltener man sein Passwort eintippt, desto besser. Deswegen sollte man sich eigentlich auch nicht ständig ab- und anmelden. Langfristig führt das dazu, dass man nicht mehr genau hinsieht, auf welcher Webseite man sich gerade befindet. So haben Passwortdiebe leichteres Spiel. Wir empfehlen unseren Nutzern deshalb, eingeloggt zu bleiben.

> » Viele Vorsichtsmaßnahmen laufen im Hintergrund ab «
>
> **Mark Risher**

Die Webseite meiner Bank loggt mich aber automatisch aus, wenn ich ein paar Minuten nicht aktiv war.

Micklitz: Es gibt leider auch viele Unternehmen, die veralteten Regeln folgen. Der Ratschlag, sich jedes Mal auszuloggen, stammt aus einer Zeit, als die meisten noch in Internetcafés online gegangen sind oder sich mit anderen einen Computer geteilt haben. Unsere Forschung zeigt: Je häufiger Menschen ihre Passwörter für einzelne Accounts eingeben, desto wahrscheinlicher werden sie Opfer eines Hackerangriffs. Deshalb ist es besser, lediglich die Bildschirmsperre Ihres Telefons oder Computers zu aktivieren und dort ein sicheres Passwort zu verwenden.

Risher: Das stimmt. Leider sind jede Menge solcher falscher oder unpraktischer Ratschläge im Umlauf. Das verwirrt die Nutzer. Im schlimmsten Fall sind sie so verunsichert, dass sie resignieren: »Ich kann mich ja sowieso nicht schützen, dann kann ich es auch gleich sein lassen.« Das ist so, als würde man die Haustür immer offen stehen lassen, weil man weiß, dass es Einbrecher gibt.

Wie würde denn Google die Sicherheit seiner Nutzer gewährleisten, wenn es keine Passwörter mehr gäbe?

Risher: Schon heute laufen viele Vorsichtsmaßnahmen im Hintergrund ab. Wenn ein Betrüger Ihr Passwort und Ihre Handynummer herausfindet, können wir die Sicherheit Ihres Google-Kontos trotzdem zu 99,9 Prozent gewährleisten. Wir überprüfen zum Beispiel, mit welchem Gerät sich jemand einloggt oder aus welchem Land. Wenn sich jemand schnell mehrmals hintereinander mit einem falschen Passwort in Ihrem Konto anmelden will, dann ist das für unsere Sicherheitssysteme ein Alarmsignal.

Micklitz: Zusätzlich haben wir den Sicherheitscheck entwickelt, mit dem jeder Nutzer seine eigenen Sicherheitseinstellungen Schritt für Schritt in seinem Google-Konto durchgehen kann. Mit dem Erweiterten Sicherheitsprogramm gehen wir sogar noch einen Schritt weiter. >

Interview: Serge Debrebant | Fotos: Conny Mirbach

Was verbirgt sich dahinter?

Micklitz: Ursprünglich wurde dieses Angebot für Personen entwickelt, die für Kriminelle von besonderem Interesse sein könnten, etwa Politiker, Geschäftsführer oder Journalisten. Mittlerweile steht es jedem offen, der sich im Internet schützen will. Nur wer einen speziellen USB-Stick oder Bluetooth-Sender bei sich trägt, erhält Zugang zu seinem geschützten Google-Konto.

> » Es fällt den Leuten manchmal schwer, die Risiken einzuschätzen «
>
> **Stephan Micklitz**

Risher: Dass das funktioniert, wissen wir aus eigener Erfahrung: Jeder Google-Mitarbeiter muss einen solchen physischen Schlüssel benutzen, damit sein Firmenkonto geschützt bleibt. Seit wir diese Sicherheitsmaßnahme eingeführt haben, hatten wir keinen einzigen Phishing-Fall mehr, der sich auf die Bestätigung des Passworts hätte zurückführen lassen. Der Schlüssel verbessert die Sicherheit des Google-Kontos dramatisch, da der potenzielle Angreifer nur Erfolg hat, wenn er den physischen Schlüssel hat — selbst wenn er das Passwort kennt. Normalerweise kann ein Internetkonto von überall auf der Welt gehackt werden. Konten, die mit einem Schlüssel geschützt sind, dagegen nicht.

Micklitz: Übrigens kann man Sicherheitsschlüssel für viele Webseiten nutzen, nicht nur im Rahmen des Erweiterten Sicherheitsprogramms. Es gibt sie für wenige Euro bei uns oder bei anderen Anbietern. Auf der Webseite g.co/advancedprotection erklären wir Details.

Wo lauern Ihrer Meinung nach heute die größten Gefahren im Netz?

Risher: Ein Problem sind die vielen Listen mit Nutzernamen und Passwörtern, die sich online finden. Unser Kollege Tadek Pietraszek und sein Team haben sechs Wochen lang das öffentlich zugängliche Internet durchforstet und 3,5 Milliarden Kombinationen von Benutzernamen und Passwörtern gefunden! Diese Daten stammen nicht von gehackten Google-Konten, sie wurden an anderen Stellen gestohlen. Weil aber viele Nutzer ihre Passwörter mehrmals nutzen, sind diese Listen auch für uns ein Problem.

Micklitz: Aus meiner Sicht ist Spear-Phishing ein Riesenproblem: Dabei schneidet ein Angreifer eine Nachricht so geschickt auf eine Person zu, dass es für das Opfer schwer wird, die betrügerische Absicht zu erkennen. Wir beobachten, dass Onlinebetrüger diese Methode immer häufiger anwenden und auch Erfolg haben.

Risher: Da gebe ich Stephan recht. Spear-Phishing ist auch gar nicht so aufwendig, wie es sich vielleicht anhört. Eine Spam-E-Mail zu personalisieren dauert oft nur ein paar Minuten. Dabei können sich die Hacker auch der Infos bedienen, die die Nutzer über sich selbst ins Netz stellen. Bei Kryptowährungen ist das zum Beispiel ein Problem: Wenn jemand preisgibt, dass er 10 000 Bitcoins besitzt, muss er sich nicht wundern, wenn er damit Betrüger anlockt ...

Micklitz: ... das ist ungefähr so, als würde ich mich mit dem Megaphon auf den Marktplatz stellen und meinen Kontostand verraten. Wer würde das machen? Niemand. Aber im Internet fällt es den Leuten manchmal schwer, die Risiken einzuschätzen.

Sind herkömmliche Spam-E-Mails noch ein Problem?

Micklitz: Es gibt nach wie vor tonnenweise Spam-Nachrichten, aber sie schaffen es nur noch selten in den Posteingang derer, die unser Mailprogramm Gmail verwenden.

Risher: Statistisch gesehen, handelt es sich bei jeder zweiten E-Mail um Spam. Die Anzahl solcher Betrugsversuche steigt nach wie vor an, aber unsere Sicherheitsteams sind in der Lage, sie automatisch zu erkennen und herauszufiltern. Das haben wir unter Kontrolle.

Auf welche Bedrohungen müssen wir uns für die Zukunft einstellen?

Risher: Die Vernetzung von Geräten und Diensten stellt uns vor große Herausforderungen. Heute sind ja nicht nur Laptops und Smartphones online, sondern auch Fernseher, Smartwatches oder Smart Speaker. Auf jedem dieser Geräte laufen unterschiedliche Apps. Damit bieten sich Hackern viele

DATENSCHUTZ IN MÜNCHEN

Google gründete seine Münchner Niederlassung 2006. Die Entwicklung in den Bereichen Sicherheit und Datenschutz ist hier angesiedelt. Das neue Gebäude, in dem Stephan Micklitz und sein Team heute arbeiten, wurde 2016 eingeweiht. Mittlerweile sind gut 700 Mitarbeiter am Standort untergebracht, rund drei Viertel arbeiten in der Entwicklung. Damit ist das Münchner Google-Büro das größte in Deutschland.

Mark Risher leitet bei Google das Produkt-Management in den Bereichen Sicherheit und Datenschutz. Sein Cybersecurity-Unternehmen »Impermium«, 2010 gegründet, wurde 2014 von Google gekauft. Seitdem ist Risher am Hauptsitz in Mountain View in Kalifornien tätig. Rechts im Bild: Ein Sicherheitsschlüssel, wie er im Programm Erweiterte Sicherheit eingesetzt wird. Er kostet nur wenige Euro und kann auf verschiedenen Webseiten genutzt werden. Mehr auf g.co/advancedprotection

Stephan Micklitz ist als Entwicklungsleiter weltweit für die Bereiche Sicherheit und Datenschutz bei Google verantwortlich. Er studierte Informatik an der TU München und arbeitet seit Ende 2007 bei Google in München. Micklitz gehört zum Vorstand der Initiative Deutschland sicher im Netz (DsiN).

unterschiedliche Angriffspunkte. Und weil die Geräte miteinander verbunden sind, können die Hacker versuchen, von einem Gerät aus auf Informationen auf anderen Geräten zuzugreifen. Für uns stellt sich die Frage: Wie können wir die Sicherheit unserer Nutzer trotz der Vielzahl neuer Nutzungsgewohnheiten gewährleisten?

Micklitz: Das fängt schon damit an, dass wir uns bei jedem Dienst fragen müssen, welche Daten wir wirklich benötigen – und welche Daten zwischen Diensten ausgetauscht werden.

Inwiefern hilft Ihnen künstliche Intelligenz, die Nutzer zu schützen?

Micklitz: Google macht schon lange von künstlicher Intelligenz Gebrauch.

Risher: Bei unserem E-Mail-Dienst Gmail haben wir von Anfang an mit solchen Technologien gearbeitet. Google hat sogar eine eigene Programmbibliothek namens TensorFlow entwickelt: Sie erleichtert Programmierern, die sich mit maschinellem Lernen beschäftigen, die Arbeit. Und vor allem Gmail profitiert davon — TensorFlow leistet wertvolle Dienste, wenn es darum geht, typische Muster zu erkennen.

Können Sie erklären, wie diese Mustererkennung funktioniert?

Risher: Nehmen wir an, es treten bei mehreren Nutzern verdächtige Ereignisse auf, die wir nicht einordnen können: Eine selbstlernende Maschine kann diese Ereignisse miteinander vergleichen und im besten Falle neue Formen des Betrugs erkennen — noch bevor sie sich online verbreitet.

Micklitz: Wobei man einschränken muss: Eine Maschine ist immer nur so intelligent wie der Mensch, der sie benutzt. Wenn ich eine Maschine mit falschen oder einseitigen Daten füttere, dann sind auch die Muster, die sie erkennt, falsch oder einseitig. Bei aller Begeisterung für die künstliche Intelligenz: Ihre Wirksamkeit hängt immer vom Menschen ab, der sie benutzt. Es liegt an ihm, die Maschine mit qualitativ hochwertigen Daten zu trainieren und die Ergebnisse anschließend zu überprüfen.

Risher: Als ich noch bei einem anderen E-Mail-Anbieter arbeitete, schrieb uns ein Bankangestellter aus Lagos. Damals waren die angeblich aus Nigeria stammenden Betrugs-E-Mails weit verbreitet, und der Mann beschwerte sich, dass seine E-Mails ständig im Spam-Ordner landen würden, obwohl er bei einer seriösen Bank arbeite. Das ist ein typischer Fall für eine falsche Verallgemeinerung innerhalb der Mustererkennung, die durch unzureichende Information entsteht. Wir haben dem Mann dann geholfen und den Algorithmus geändert.

WEBFITNESS

Deutschland sicher im Netz e.V. (DsiN)

WER STECKT DAHINTER?

Der Verein wurde vor 13 Jahren beim ersten Nationalen IT-Gipfel gegründet und steht unter der Schirmherrschaft des Bundesministeriums des Innern. DsiN versteht sich als Ansprechpartner für Verbraucherinnen und Verbraucher sowie kleine und mittelständische Unternehmen bei Fragen zur IT-Sicherheit.

WAS MACHT DIE ORGANISATION?

DsiN leistet Aufklärungsarbeit und will die digitale Kompetenz in der Bevölkerung fördern. Dies geschieht nicht nur auf der zugehörigen Webseite, sondern auch über Projekte für Schülerinnen und Schüler, Seniorinnen und Senioren oder Ehrenamtliche. Darüber hinaus organisiert DsiN Wettbewerbe wie »myDigitalWorld«, bei denen Jugendliche für ihre Ideen und Projekte zur Netzsicherheit ausgezeichnet werden. Mit dem sogenannten IT-Fitnesstest kann jeder ganz einfach sein Sicherheitsverhalten prüfen.

WO KANN ICH MEHR ERFAHREN?

sicher-im-netz.de

DsiN Deutschland sicher im Netz

AUF DER SICHEREN SEITE

Wie Sie mit Google Ihre Online-Sicherheit noch weiter verbessern können

Privatsphärecheck

Diese Anwendung führt Google-Nutzer durch die wichtigsten Einstellungen zum Datenschutz. Jeder kann selbst festlegen, welche Web- und App-Aktivitäten gespeichert werden sollen oder ob zum Beispiel der Google Assistant Sprachbefehle aufzeichnen darf, um die Spracherkennung zu verbessern. Mehr auf **g.co/privatsphaerecheck**

Bestätigung in zwei Schritten

Um sein Google-Konto besser vor Hackern zu schützen, kann jeder Nutzer die sogenannte Zwei-Faktor-Authentifizierung verwenden. Für die Anmeldung bei Google muss dazu zusätzlich zum Passwort ein Bestätigungscode eingetippt werden, der per SMS oder Telefonanruf übermittelt wird. Alternativ kann jeder auch einen Code über den Google Authenticator generieren oder einen Sicherheitsschlüssel benutzen. Mehr auf **g.co/2step**

Personalisierung von Anzeigen

In den »Einstellungen für Werbung« im Google-Konto können Nutzer entscheiden, inwiefern Google personenbezogene Daten verwenden darf, um Anzeigen auszuwählen, die für die jeweilige Person interessant und nützlich sind. Google analysiert diese Informationen und leitet, zum Beispiel, Themengebiete wie »Fahrzeuge« oder »Fitness« ab. Wer ganz auf personalisierte Werbung verzichten möchte, kann diese abschalten und generische Anzeigen erhalten. Übrigens gibt Google diese Daten nicht an andere Unternehmen oder Organisationen weiter. Mehr auf **g.co/einstellungenfuerwerbung**

Sicherheitscheck

Wer sein Konto schützen will, braucht dafür nur wenige Minuten. Schritt für Schritt führt der Sicherheitscheck jeden Nutzer durch die wichtigsten Einstellungen, um die Sicherheit des Google-Kontos zu erhöhen: Sie erhalten Hinweise dazu, ob Google die Apps von Drittanbietern als sicher einstuft, welche Geräte angemeldet sind oder welche sicherheitsrelevanten Ereignisse zuletzt aufgetreten sind. Wichtig: Jeder kann hier eine zweite E-Mail-Adresse und eine Telefonnummer hinterlegen, über die Google den Nutzer bei verdächtigen Aktivitäten erreichen kann. Mehr Infos auf **g.co/sicherheitscheck**

Erweiterte Sicherheit

Mit dem Erweiterten Sicherheitsprogramm spricht Google Menschen an, die im Netz besonders gefährdet sind, gehackt zu werden. Dazu gehören zum Beispiel Politiker oder Journalisten. Zentraler Bestandteil des Angebots ist die Zwei-Faktor-Authentifizierung mit physischem Schlüssel: Nur wer einen speziellen USB-Stick oder Bluetooth-Sender bei sich trägt, erhält Zugang zum geschützten Google-Konto. Mehr auf **g.co/advancedprotection**

Mehr Informationen auf
g.co/sicherheitscenter

Google Pay

Mit dem Bezahldienst Google Pay können Nutzer in Deutschland nicht nur in Apps oder auf Webseiten einkaufen, sondern auch per Smartphone an der Ladenkasse bezahlen. Dafür hinterlegen die Nutzer ihre Zahlungsinformationen (zum Beispiel für die Kreditkarte einer teilnehmenden Bank oder für ein PayPal-Konto) bei Google Pay. Am Bezahlterminal wird dann keine Kreditkartennummer übermittelt, sondern eine verschlüsselte Ziffernfolge, der sogenannte Token. Dieses Verfahren macht Google Pay sicherer als Kreditkarten. Mehr auf **pay.google.com**

Passwort-Warnungen

Google verschickt automatisch einen Hinweis, sobald sich ein Nutzer von einem neuen Gerät oder aus einem anderen Land anmeldet. Eine Erweiterung des Browsers Chrome reagiert, sobald ein Nutzer sein Google-Passwort auf der falschen Webseite eingibt. Dazu prüft das Programm, ob die jeweilige Webseite zu Google gehört. Erscheint ein Warnhinweis, sollte der Nutzer sein Passwort ändern, um sein Google-Konto zu schützen. Mehr auf **chrome.google.com**

Google-Konto

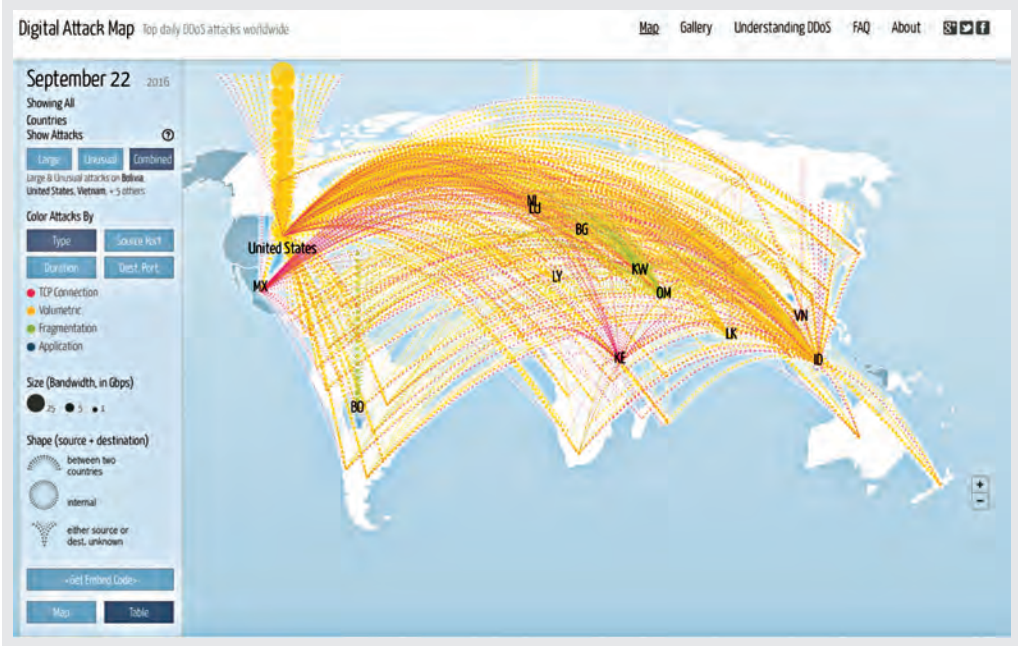
Hier sind viele Informationen und Einstellungen zu Sicherheit und Datenschutz gebündelt. Google-Nutzer erhalten an diesem Ort einen Überblick zu den Daten, die Google speichert, und können bestimmen, welche Informationen in Zukunft erfasst werden sollen. Sie können auch beeinflussen, welche Werbung Google ihnen zeigt. Mit dem Privatsphäre- und dem Sicherheitscheck kann jeder seine Einstellungen überprüfen. Wer will, kann die dort angezeigten Aktivitätsdaten löschen. Mehr auf **meinkonto.google.de**

Text: Serge Debrebant | Illustrationen: Robert Samuel Hanson

»Kein Land ist immun«: Jamie Albers entwickelt mit ihren Kollegen Ideen für die Abwehr digitaler Angriffe.

Die können helfen

Für Informationsfreiheit und faire Wahlen, gegen Terror-Propaganda und Korruption: Mit digitalen Technologien hilft die Google-Initiative Jigsaw, Menschen auf der ganzen Welt vor Bedrohungen zu schützen



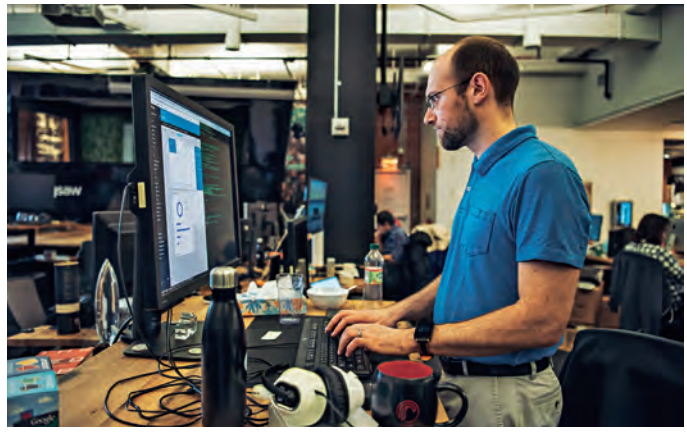
Die Digital Attack Map zeigt auf einer öffentlich zugänglichen Karte die schwersten DDoS-Angriffe an, die gerade auf der Welt stattfinden: digitalattackmap.com

WENN IM MAI 2019 über die künftige Zusammensetzung des Europäischen Parlaments abgestimmt wird, geschieht das mit einer der größten demokratischen Wahlen der Welt: Rund 400 Millionen Wahlberechtigte aus 27 Staaten dürfen 705 Abgeordnete bestimmen, die die Interessen der Bürger in Brüssel und Straßburg vertreten. Noch viel mehr als bei vorangegangenen Europawahlen wird dieses Jahr die Sicherheit der Abstimmung eine Rolle spielen. »Alle Mitgliedstaaten müssen die Bedrohung der demokratischen Prozesse und Institutionen durch Cyberangriffe und Desinformationen ernst nehmen«, warnte EU-Sicherheitskommissar Julian Kling kürzlich vor Manipulation und Einflussnahme auf die Wahl.

Jigsaw schützt Webseiten vor DDoS-Attacken

Jamie Albers hält solche Sorgen für durchaus berechtigt. »Kein Land ist immun gegen diese Probleme«, sagt die Frau, die sich seit 2016 intensiv mit dem Schutz von Wahlen in aller Welt beschäftigt. Albers arbeitet in New York und verantwortet das Marketing bei Jigsaw (Deutsch: »Puzzle«), einem Innovationszentrum des Google-Mutterkonzerns Alphabet. Rund 60 Mitarbeiter entwickeln dort Technologien, die Menschen vor Gefahren und Einschränkungen in der Online- und Offlinewelt schützen sollen. Ihre digitalen Werkzeuge unterstützen Engagierte rund um den Globus dabei, gegen Cybermobbing oder Korruption, gegen Geldwäsche, terroristische Propaganda oder gegen die Einschränkung der Meinungs- und Informationsfreiheit zu kämpfen.

Seit einiger Zeit beobachten Jamie Albers und ihr Team zum Beispiel, dass gerade in Wahlkampfzeiten feindselige Aktivitäten im Internet zunehmen. Albers kam 2016 in Ecuador mit dem Problem in Berührung: Politische Journalisten und Aktivisten berichteten von massiven Behinderungen ihrer Arbeit durch Phishing-Angriffe, bei denen vertrauliche Daten ausgespäht wurden. Außerdem erzählten sie von sogenannten DDoS-Attacken. Das Kürzel steht für »Distributed Denial of Service« und beschreibt eine erschreckend günstige Methode, um beispielsweise Journalisten mundtot zu machen: Für 20 Euro lässt sich eine Nachrichtenwebseite mit massenhaften, sinnlosen Anfragen überfluten und dadurch lahmlegen. In Südamerika erfuhr Jamie Albers



Im New Yorker Stadtteil Chelsea arbeiten Techniker und Politikexperten bei Jigsaw an Schutzmechanismen für die digitale Welt.

Text: Christoph Henn | Fotos: Reto Sterchi

auch, dass es infolge gezielter Belästigungen in Ecuador kaum mehr investigative Journalisten gibt. »Wir fanden außerdem heraus, dass einige Monate vor der Wahl ganze Armeen von Chat-Robotern in Kommentarbereichen und Onlineforen unterwegs waren, um mit Provokationen die öffentliche Debatte zu beeinflussen.«

Jamie Albers begann, verschiedene digitale Sicherheitswerkzeuge zu entwickeln. Zusammengenommen nennt sie diese »Protect Your Election«, zu Deutsch: Schütze deine Wahl. Es handelt sich um kostenlose Programme, die Journalisten, Nichtregierungsorganisationen und Menschen helfen können, die sich auf ihren Webseiten mit Informationen zu Wahlen befassen. Mithilfe des Programms »Erweiterte Sicherheit« zum Beispiel lassen sich Onlinekonten vor unbefugten Zugriffen schützen. »Project Shield« schirmt Internetseiten gegen DDoS-Angriffe ab. Die von Jigsaw entwickelte Programmierschnittstelle »Perspective« unterstützt die Moderatoren von Kommentarbereichen dabei, eine offene, respektvolle Diskussionskultur sicherzustellen: Sie erleichtert das Erkennen von Beleidigungen und Belästigungen in Onlinediskussionen.

Häufig recherchieren Jigsaw-Mitarbeiter an Brennpunkten in aller Welt und entwickeln dann im New Yorker Büro digitale Problemlösungen.

Albers und Kollegen beschäftigen sich mit geopolitischen Herausforderungen

Die beschriebenen Gefahren gibt es nicht nur in Ecuador. Im US-Wahlkampf 2016 wurde die demokratische Partei Opfer einer großen Phishing-Attacke. Und kurz vor der niederländischen Parlamentswahl 2017 meldete sich ein Kollege aus Amsterdam bei Jamie Albers: Zwei der wichtigsten Informationsseiten zur Wahl waren nach DDoS-Attacken nicht mehr abrufbar. »Spätestens da war klar, dass wir ›Protect Your Election‹ weltweit verfügbar machen müssen«, erinnert sich Albers. Inzwischen gibt es ihr Programm in mehr als 20 Ländern, und es hilft dabei, dass Menschen ungehindert auf wahlrelevante Informationen im Internet zugreifen können.

Ehe die Jigsaw-Mitarbeiter im New Yorker Stadtteil Chelsea ihre modernen Büros mit bunten Sitzmöbeln, eleganten Lounges und Schlafkabinen für Power Naps betreten, begegnen sie im Foyer an der Wand einer Frage, formuliert in übergroßen Lettern: »Wie kann Technologie den Menschen zu einer sichereren Welt verhelfen?« Tag für Tag arbeiten Techniker, Produktmanager, Designer, Forscher, Politik- und Marketingexperten bei Jigsaw an einer Antwort. Die Mitarbeiter stammen nicht nur aus den USA, sondern auch aus Südamerika und Europa oder aus dem Nahen Osten. Sie bringen unterschiedlichste Perspektiven mit, wenn sie in wechselnden Teams Bedrohungen identifizieren, über mögliche Gegenmittel nachdenken und schließlich die entsprechenden Technologien programmieren und veröffentlichen.

In der New Yorker Zentrale findet aber nur ein Teil der Arbeit statt. So oft es geht, recherchieren die Jigsaw-Mitarbeiter an Brennpunkten in aller Welt. In der Vergangenheit sprachen sie im Irak mit IS-Aussteigern über die Onlinerekrutierungsstrategien der Terrororganisation oder tauschten sich in Mazedonien mit »Trolls« aus, die hinter gezielten Desinformationskampagnen in sozialen Medien stehen. Meist beschäftigen sich Jamie Albers und ihre Kollegen bei ihrer Forschung mit geopolitischen Herausforderungen, die in der öffentlichen Wahrnehmung noch gar nicht existieren. »Meine Aufgabe ist es dann, ein Bewusstsein zu schaffen und das Problem verständlich zu machen«, sagt Jamie Albers. Zurzeit arbeitet sie schon wieder an einem neuen Projekt. Allerdings noch im Geheimen, wie so oft.

AKTUELLE JIGSAW-PROJEKTE

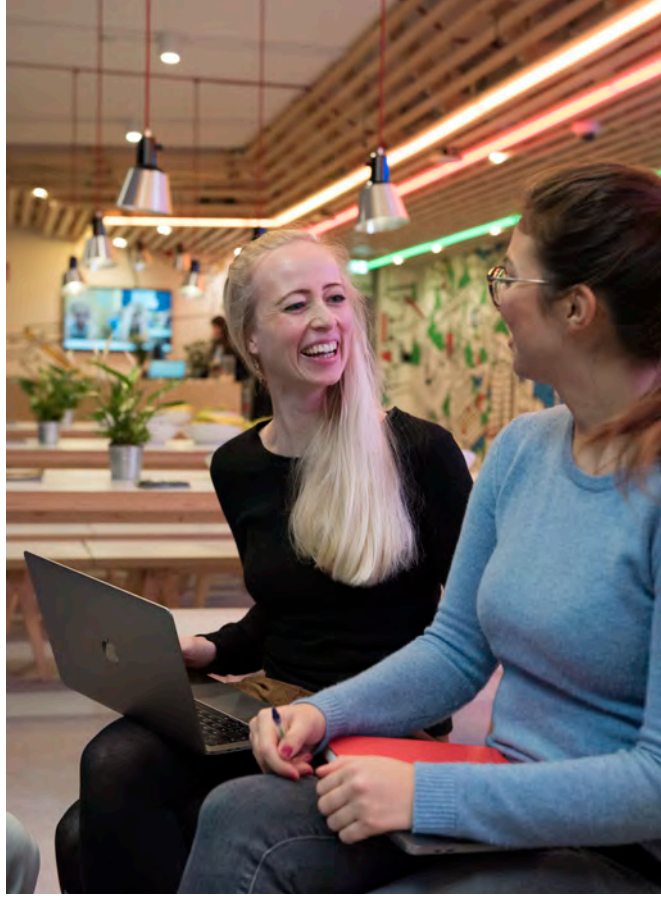
Unfiltered News zeigt mithilfe von Google News, welche Nachrichten in einem Land weniger abgedeckt werden als in anderen Teilen der Welt. **unfiltered.news**

Project Shield verwendet die Infrastruktur von Google, um zum Beispiel unabhängige Nachrichtenwebseiten oder die Onlineangebote von Menschenrechtsorganisationen vor DDoS-Angriffen zu schützen: Bei solchen Attacken werden Internetseiten absichtlich mit einer großen Zahl von Anfragen überfrachtet. Project Shield bietet den Schutz vor DDoS-Angriffen auch in Europa, wo vom 23. bis 26. Mai 2019 das Parlament gewählt wird. Organisationen oder Webseitenverantwortliche, die im Vorfeld Angriffe befürchten, können sich auf **projectshield.withgoogle.com** registrieren. Dort erfahren sie alles Weitere dazu, wie Project Shield Angebote schützen kann.

Perspective unterstützt Moderatoren dabei, eine offene und respektvolle Diskussionskultur in Internetforen sicherzustellen. **perspectiveapi.com**

Password Alert benachrichtigt Nutzer, wenn eine Webseite versucht, ihr Passwort zu stehlen. **chrome.google.com/webstore/detail/password-alert**

Outline versorgt Nachrichtenmedien mit einem geschützten VPN-Zugang, damit Journalisten online sicher recherchieren und kommunizieren können. **getoutline.org**



Lena Rohou und ihr Team vermitteln mit der Google Zukunftswerkstatt in ganz Deutschland digitales Know-how.

Lena Rohou von Google verantwortet **das Programm der Google Zukunftswerkstatt,** in der auch Trainings zum Thema Datensicherheit angeboten werden

» Sicher durch die Onlinewelt «

Frau Rohou, Kompetenzen in Datenschutz und Datensicherheit sind für Privatpersonen und Unternehmen gleichermaßen relevant. Welche Trainings bieten Sie dazu an?

In der Google Zukunftswerkstatt trainieren wir digitale Kompetenzen, egal, ob nun für die persönliche Karriere oder zur Weiterentwicklung eines Unternehmens. Die Spanne an Themen reicht von den Grundlagen des Onlinemarketing bis hin zu Methoden des agilen Arbeitens. In unseren Trainings zu Datenschutz und Datensicherheit erklären wir die Zwei-Schritt-Authentifizierung, also die Account-Anmeldung in zwei Etappen. Wir vermitteln auch, was Phishing ist und wie man sich davor schützt. Unternehmer lernen in der Zukunftswerkstatt unter anderem die Integration von HTTPS auf Webseiten.

Fotos: Eva Häberle, Angela Regenbrecht

Wie laufen die Kurse ab?

Alle Angebote sind kostenlos — ganz egal, ob Sie sich zu einem Training an einem unserer Standorte in München, Hamburg oder Berlin anmelden oder die Onlineplattform auf Zukunftswerkstatt.de nutzen. Jedes Vor-Ort-Training dauert in etwa zwei Stunden. Das Schöne dabei: Sie haben die Gelegenheit, Kontakte zu den anderen Teilnehmern zu knüpfen und sich auszutauschen.

Welche neuen Fähigkeiten nehmen die Teilnehmer mit nach Hause?

Natürlich wird in zwei Stunden niemand zum Experten. Aber die Zeit reicht aus, um Grundlagen zu verstehen und ein gutes Gespür dafür zu entwickeln, wie man sich privat und beruflich sicher durch die Onlinewelt bewegt.

Jetzt anmelden und mitmachen

Das digitale Zeitalter kann kommen: Mit den kostenlosen Trainings der Google Zukunftswerkstatt können sich Menschen beruflich und persönlich weiterentwickeln – vor Ort und online auf **Zukunftswerkstatt.de**. Hier eine kleine Auswahl der Themen:

Online-Kommunikation:
Über welche Kanäle erreiche ich meine Kunden?

#IamRemarkable:
Selbstbewusst über Erfolge sprechen

Sicher durchs Web:
Grundlagen zu Datenschutz und Datensicherheit

Alle weiteren Informationen auf **Zukunftswerkstatt.de**

HINTER DEN KULISSEN

Wie Google sich dafür einsetzt, dass Sie sich online sicher bewegen können

Verschlüsselung

Google setzt unterschiedliche Verschlüsselungstechnologien wie HTTPS oder Transport Layer Security ein, wenn zum Beispiel E-Mails via Gmail verschickt werden oder wenn Nutzer Fotos in der Cloud speichern. Auch Googles Suchmaschine ist standardmäßig mit HTTPS verschlüsselt.

Infrastruktur

Google betreibt eine der größten und sichersten Cloud-Infrastrukturen der Welt. Die Rechenzentren befinden sich auf der ganzen Welt und sind per Unterwasser-Glasfaserkabel über Kontinente hinweg miteinander verbunden. Dieses System wird rund um die Uhr bewacht.

Google Play Protect

Jeden Tag testet dieses Schutzprogramm rund 50 Milliarden Android-Apps auf Schadprogramme und Viren. Die erste Überprüfung erfolgt, wenn ein Anbieter eine App in den Google Play Store einzustellen versucht. Auch wenn Nutzer eine App herunterladen wollen oder auf ihrem Endgerät verwenden, wird sie von Google Play Protect kontrolliert. Entdeckt das Sicherheitsprogramm schädliche oder verdächtige Software, warnt Google den Nutzer oder entfernt die App automatisch. Mehr Informationen auf **android.com**

Prüfen von Anfragen

Google gewährt Geheimdiensten oder anderen Regierungseinrichtungen keinen direkten Zugriff auf Nutzerdaten. Das gilt für die USA genauso wie für Deutschland und jedes andere Land der Welt. Fragt eine Behörde Daten eines Nutzers an, wird diese Anfrage von Google geprüft und zurückgewiesen, falls sie unbegründet ist. Zu Datenanfragen veröffentlicht Google seit Jahren Transparenzberichte unter **transparencyreport.google.com**

Sicheres Surfen

Die »Safe Browsing«-Technologie schützt Nutzer vor Betrugsversuchen und Schadprogrammen im Internet. Im Kern besteht sie aus einer Datenbank mit den Adressen verdächtiger Webseiten. Will ein Nutzer eine dieser Webseiten ansteuern, erhält er eine Warnung. Um neuartigen Phishing-Tricks zuvorzukommen, setzt Google zudem auf künstliche Intelligenz. Mehr dazu auf **safebrowsing.google.com**

Lücken schließen

Jedes Jahr fließen viele Millionen Dollar in Forschungsprojekte und sogenannte Bug Bounties – das sind Finderlöhne für Experten, die dem Unternehmen bislang unentdeckte Sicherheitslücken melden. Der 18-jährige Uruguayer Ezequiel Pereira half Google bereits mehrmals, solche Lücken zu entdecken. Einer seiner Hinweise wurde im vergangenen Jahr 2018 mit einer Prämie von 36 337 Dollar belohnt.

Project Zero

Googles Eliteeinheit in Sachen Sicherheit konzentriert sich darauf, Sicherheitslücken zu schließen, ehe Hacker und Datendiebe sie finden. Solche Lücken nennen Experten auch »Zero Day Vulnerabilities« — daher auch der Name der Abteilung, »Project Zero«. Das Team konzentriert sich übrigens nicht allein auf Google-Dienste, es versucht auch, Schwachstellen bei Mitbewerbern zu entdecken und diese zu informieren, um Nutzer zu schützen. Weitere Informationen zur Arbeit von Project Zero auf **googleprojectzero.blogspot.com**

Im Einsatz für andere IT-Anbieter

Immer wieder stellt Google seine Sicherheitstechnologien auch anderen Unternehmen kostenlos zur Verfügung, um das Internet auch außerhalb des Google-Universums sicherer zu gestalten. So können Entwickler anderer Firmen den Cloud Security Scanner nutzen, um Sicherheitslücken zu untersuchen. Googles »Safe Browsing«-Technologie ist auch im Safari-Browser von Apple und im Mozilla Firefox im Einsatz.

Spam-Schutz durch künstliche Intelligenz

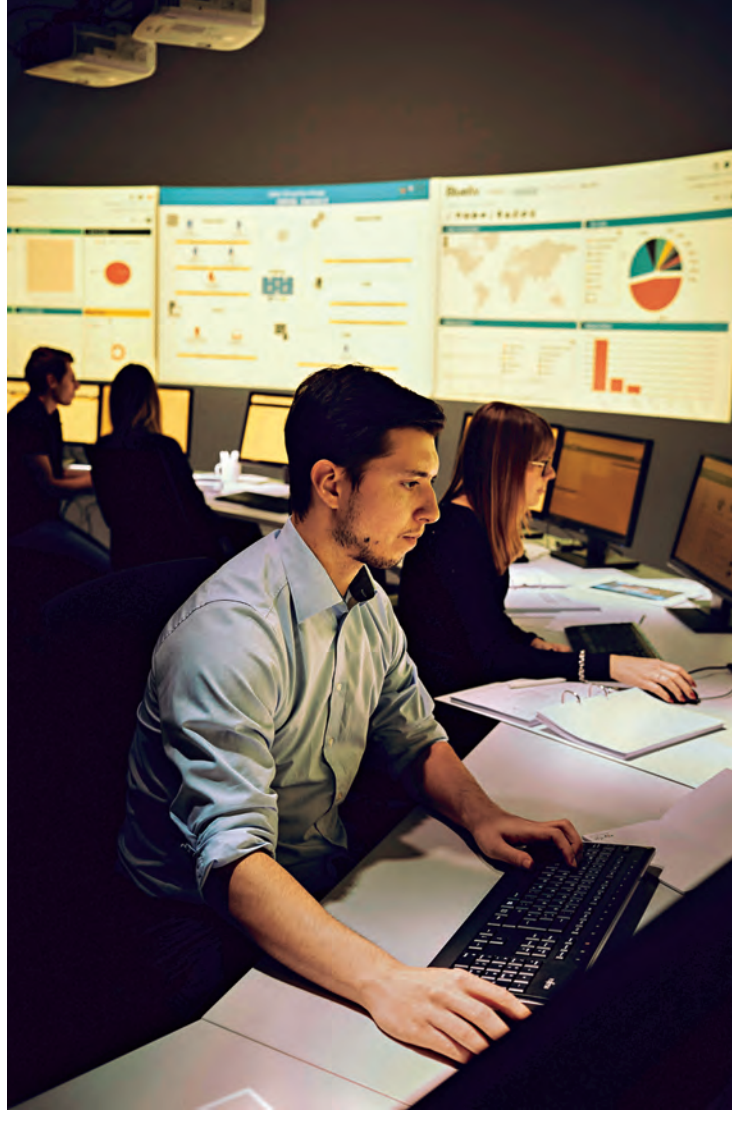
Um Gmail-Nutzer vor Spam zu schützen, analysiert Google Betrugsversuche mithilfe von maschinellen Lernverfahren: Neuronale Netzwerke prüfen Milliarden von E-Mails und leiten Muster ab, mit deren Hilfe sie unerwünschte Spam-E-Mails identifizieren. Der Erfolg gibt Google Recht. Heute landen weniger als ein Promille aller Spam-E-Mails im Posteingang – und täglich werden es weniger.

Mehr Informationen auf
g.co/sicherheitscenter

Text: Serge Debrebant | Illustrationen: Robert Samuel Hanson

Im Information Security Hub des Münchner Flughafens **wappnen sich Unternehmen** unter realistischen Bedingungen und auf neutralem Boden gegen Cyberattacken. Ein Besuch

Den Ernstfall üben



Risiken verstehen, Verteidigung üben: Ein Blick in das Innere des Information Security Hub.

ALLES UNTER KONTROLLE im Control-Center. Oder etwa nicht? Auf einer 180-Grad-Leinwand, die einen großen Teil des Raums einnimmt, leuchtet jetzt ein seltsames Bild aus Kommata, Punkten, Zahlenfragmenten und einzelnen Wörtern auf. Die Spuren eines Cyberangriffs. »Und, was sagt uns das jetzt?«, fragt Pierre Kroma in eine Runde aus vier Herren, die mit ernsten Gesichtern vor dem ansonsten dunklen Halbrund sitzen. »Der Attacker ist eine Maschine«, kommt die erste Antwort. Und weiter: »Wenn er im gleichen Subnet ist und es keinen Gatewaytraffic gibt, sind wir geliefert.«

Will »die Guten« zu mehr Kooperation bewegen: IT-Security-Experte Marc Lindike

Die vier Herren, die diese kryptische Technikspache sprechen und verstehen, sind Cyberanalysten bei einem großen deutschen Unternehmen, das sehr sensible Daten verwaltet. Ein möglicher Diebstahl dieser Daten hätte katastrophale Folgen. Damit die IT einen digitalen Angriff rechtzeitig erkennt, möglichst gut abwehren oder den Schaden zumindest begrenzen kann, trainieren die vier Spezialisten im Information Security Hub (ISH) am Münchner Flughafen den Ernstfall. Pierre Kroma, ein sogenannter guter Hacker, unterrichtet sie in Cyberverteidigung.

Dass es diesen Ort gibt, an dem der Ernstfall unter kundiger Anleitung und möglichst realistischen Bedingungen trainiert werden kann, ist Marc Lindike zu verdanken. Der IT-Security-Chef des Münchner Flughafens rüstete die ehemalige Postverteilstelle des Unternehmens gemeinsam mit drei Kooperationspartnern zu einer fiktiven Referenzfirma mit allen Finessen um: Hunderte Server, Netzwerkclients und Kameras wurden verbaut. Seit der Eröffnung des ISH im Januar 2018 simulieren Dax-Unternehmen, Mittelständler oder auch Behörden an diesem Ort Cyberattacken jeder Art. Die Übungen werden für jede Firma individuell inszeniert; selbst Fertigungsstraßen und Roboter lassen sich, je nach Bedarf, in die Szenarien integrieren.

Um die realen Auswirkungen eines Cyberkrieges zu vermitteln, greifen die Macher des ISH zu mitunter drastischen Mitteln. Im »Amphitheater«, dem Zentrum des Hubs mit großer Leinwand und Platz für 140 Menschen, startet Lindike eine kleine »Horrorshow«. Das Stroboskop blitzt, ein ohrenbetäubender Musikmix aus Songs von Helene Fischer, The Prodigy und der Metalband Disturbed dröhnt aus den Laut-

Text: Elisa Holz | Fotos: Conny Mirbach

sprechern, man hört Menschen schreien. »Da gibt jeder sein Bestes, damit das schnellstmöglich aufhört«, sagt Marc Lindike und grinst. Cyberdrill heißt diese praxisorientierte Abhärtungsmethode im Fachjargon. Lindike hält sie auch keineswegs für übertrieben: In der IT-Security müsse man schnell, präzise und vor allem unter Hochdruck arbeiten können. Niemand soll während des Trainings in falscher Sicherheit gewogen werden. Allein der Flughafen München, so Marc Lindike, müsse jeden Tag Zigtausende von digitalen Viren und Würmern abwehren. Bis zu viermal pro Woche wird die »national kritische Infrastruktur«, als die der Flughafen eingestuft ist, gezielt angegriffen.

Die Bösen arbeiten schon zusammen, die Guten noch nicht

Im Angesicht dieser Zahlen sitzt Michael Zaddach, IT-Chef des Flughafens, relativ entspannt in seinem Büro mit Blick auf Terminals und Tower. Jeden Tag starten und landen hier 150 000 Menschen. Eine logistische Meisterleistung, die ohne eine reibungslos funktionierende Informationstechnik nicht möglich wäre. Für Zaddach sind die gut fünf Millionen Euro für das »Projekt ISH« deshalb nicht zuletzt ein Investment in eigener Sache. Auch die Mitarbeiter des Hauses sollen hier trainieren, sollen sich weiterbilden und mit Security-Experten anderer Branchen zusammenarbeiten.

Für Zaddach ist Kooperation das Gebot der Stunde. Mit der fortschreitenden Digitalisierung wird die ohnehin schon komplexe IT-Architektur des Flughafens noch komplexer und damit verwundbarer, was Cyberterroristen, Erpressern oder auch staatlichen Geheimdiensten in die Hände spielt. »Deshalb müssen wir uns besser vernetzen«, sagt der IT-Chef des Flughafens. »Am besten über Branchen- und Ländergrenzen hinweg.« Das ISH soll dabei ein Dreh- und Angelpunkt der europäischen Cybersecurity-Szene werden. Im Mai zum Beispiel findet dort eine große Sicherheitskonferenz statt, zu der unter anderem auch der russische Computervirologe Jewgeni Kasperski kommen wird.

Übungsplatz für den Cyberwar: das ISH am Münchner Flughafen. Mehr Informationen auf ish-muc.com

»Wir sind hier wie die Schweiz«, erklärt Marc Lindike. »Mit dem ISH sind wir ein neutraler Boden, auf dem sich alle treffen und austauschen können.« So eine Schweiz scheint auch dringend nötig. Denn sobald es um IT-Sicherheit geht, halten viele Unternehmen hinterm Berg. Dabei haben alle die gleichen Probleme: Es fehlt an Fachkräften, an Ressourcen, und es fehlt das Bewusstsein für die wachsenden Gefahren des real existierenden Cyberwars. Um dieses Bewusstsein zu schaffen, braucht es Raum. Deshalb sind die 1500 Quadratmeter in dem unauffälligen Bürogebäude, in dem das ISH residiert, nicht nur ein »Truppenübungsplatz für Cyberwar« wie Lindike sagt. Das Hub soll vor allem eine Plattform sein, auf der Security-Experten mit Gleichgesinnten das notwendige Wissen erarbeiten, von den Grundlagen bis zur Anwendung. »Die Bösen arbeiten schon zusammen, die Guten noch nicht«, sagt Marc Lindike. Das ändert sich unter anderem mit Angeboten wie dem ISH.

AMTSHILFE

Bundesamt für Sicherheit in der Informationstechnik (BSI)

WER STECKT DAHINTER?

Die Behörde wurde 1991 gegründet und ist dem Bundesministerium des Inneren unterstellt. Rund 1000 Mitarbeiter befassen sich hier mit Fragen der IT-Sicherheit.

WAS MACHT DIE ORGANISATION?

Das BSI kümmert sich um die »Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft«. Zu seinen Aufgaben gehören der Schutz der staatlichen IT vor Netzangriffen, die Entwicklung von Standards und Zertifizierungen und der Verbraucherschutz. Die Webseite des BSI gibt einen umfassenden Überblick zum Thema Netzsicherheit — vom sicheren Onlinebanking bis hin zu Empfehlungen für ein sicheres WLAN. Außerdem unterstützt das BSI eine Reihe von Projekten, um die Digitalkompetenz der Menschen zu fördern.

WO KANN ICH MEHR ERFAHREN?

Telefonberatung: 0800 274 1000
E-Mail: mail@bsi-fuer-buerger.de
bsi-fuer-buerger.de

Bundesamt für Sicherheit in der Informationstechnik

Stephan Somogyi macht im Security and Privacy Produktmanagement von Google **unser digitales Leben sicherer.** Er sagt: Wir müssen lernen, im Umgang mit dem Netz kritischer zu denken

»Wir wollen anderen vertrauen«

Herr Somogyi, wir sind rundum versichert, schnallen uns beim Autofahren an und verdecken unsere PIN am Geldautomaten. Warum sind wir im Internet so sorglos?

Das ist nicht nur ein deutsches, sondern ein globales Phänomen. Ursache ist die menschliche Psyche. Wir setzen uns leichter mit konkreten und sichtbaren Gefahren auseinander. Das ist im Internet nicht der Fall. Umso wichtiger ist es, dass wir Tech-Firmen dafür sorgen, dass die Nutzer sicher sind. Entsprechend intensiv haben wir in den vergangenen Jahren daran gearbeitet.

An welchen Stellschrauben haben Sie gedreht?

Wir haben viel Zeit und Geld investiert, unsere Nutzer besser zu verstehen. Wir konnten zum Beispiel feststellen, dass früher zu viele Sicherheitswarnungen angezeigt wurden. Das führte dazu, dass die Leute diese nicht mehr ernst genommen haben. Also stellt sich die Frage: Wie viel ist gerade richtig? Es ist nicht einfach, hier das rechte Maß zu finden. Der Faktor Mensch wird zumeist unterschätzt.

Wie meinen Sie das?

Wenn sich der Nutzer aktiv dafür entscheidet, auf einen Link in einer E-Mail zu klicken oder Daten unbedacht preiszugeben, wird es schwierig. Die meisten Angriffe zielen darum auf die Gutgläubigkeit des Menschen.

Das bedeutet?

Wir Menschen sind so gestrickt, dass wir anderen vertrauen wollen. Das wissen die Kriminellen. Sie versuchen uns deshalb, dazu zu bringen, einer wildfremden E-Mail zu trauen — oder die Angreifer machen uns schlicht Angst, um uns zu verunsichern. Die Folge ist in beiden Fällen dieselbe: Wir treffen eine schlechte Entscheidung.

Können Sie ein Beispiel nennen?

Stellen Sie sich vor, in Ihrem Postfach taucht die Nachricht auf, dass der Video-Streaming-Dienst, über den man sich die neue Folge der Lieblingsserie anschauen wollte, gesperrt werden soll. Um das zu verhindern, müsse man auf den folgenden Link klicken und die aktuellen Bankdaten bestätigen. Viele Menschen entscheiden sich in einem solchen Moment falsch und folgen einem solchen Hinweis. Und schon sitzt irgendjemand in ihrem Konto.

Die Angreifer wollen Nutzer also immer zu einer unbedarften Aktion reizen?

Ja. Es gibt aber auch viele Fälle, in denen aus Unwissen oder Bequemlichkeit einfach Sicherheitswarnungen ignoriert werden. Wir arbeiten deshalb daran, die Benutzerführung bei Warnhinweisen zu vereinfachen. Wir wollen dem Nutzer nicht vorschreiben, was er zu tun oder zu lassen hat. Er soll aber wissen, dass es ab bestimmten Punkten gefährlich werden kann. Wir wollen ihm alle Infos bieten, die er für seine Entscheidung braucht – aber auch nur die.

Menschlicher Faktor: Stephan Somogyi beschäftigt sich mit unserem Verhalten im Web.

Für viele ist der stationäre Rechner nicht mehr erste Wahl. Unterscheiden sich die Sicherheitsanforderungen für die unterschiedlichen Endgeräte?

Das ist für uns eine große Herausforderung, gerade weil mobile Daten für die Nutzer teurer sind. Auf einem stationären Rechner, der sich die Daten meist nicht über das Mobilnetz holt, spielt dies eher keine Rolle — auf dem Smartphone wegen des Datenvolumens möglicherweise schon. Als wir unser Safe Browsing System, das auch von Browsern wie Firefox, Safari und Chrome genutzt wird, auf Handys erweitert haben, mussten wir dies alles berücksichtigen. Alle zur erhöhten Sicherheit erforderlichen zusätzlichen Daten müssen deshalb nachweisbar zweckdienlich sein. Wir haben den Datentransfer bei mobilen Endgeräten nun auf ein Viertel reduziert. Schließlich wollen wir nicht, dass Kunden Schutzmaßnahmen ausschalten, nur weil sie ihr Datenvolumen schonen wollen. Auch hier kommen der Mensch und sein Ermessen ins Spiel.

Angenommen, man folgt den Sicherheitshinweisen und ist auch sonst vorsichtig mit seinen Daten – was heißt das für externe Virenprogramme? Kann ich mir die sparen?

Sagen wir es so: Wenn Sie Ihr System konsequent aktualisieren und auf dem neuesten Stand halten, sind Sie heutzutage gut geschützt. Das war nicht immer der Fall. Viele Unternehmen kümmerten sich in der Vergangenheit nicht in der nötigen Gründlichkeit um dieses Thema. Da wurde in den vergangenen Jahren nachgelegt.

Noch ein kurzer Blick in die Zukunft. Welches Ziel gehen Sie als Nächstes an?

Der Standard HTTPS soll sich im ganzen Netz noch weiter etablieren, damit Verbindungen stets verschlüsselt sind. Schon heute verwenden wir für viele unserer Dienste, zum Beispiel die Google-Suche oder Gmail, ausschließlich sichere HTTPS-Verbindungen zum Übertragen von Daten.

Alle Daten im Netz sollen sicher übertragen werden?

Ja. Bisher werden sichere Verbindungen in der Adressleiste eigens ausgewiesen. Das wollen wir umdrehen: Künftig soll stattdessen jede unsichere Verbindung gekennzeichnet sein, damit man das Risiko besser erkennt.

Interview: Dominik Wüchner | Foto: Felix Brüggemann

NA SICHER

Mit diesen Tipps bewegen Sie sich risikofreier durchs Internet

Jedes Passwort nur einmal verwenden

Sonst sind gleich mehrere Accounts gefährdet, falls ein Angreifer Ihr Passwort herausfindet.

Regelmäßig Sicherheitsupdates installieren

Damit keine Lücken für Angreifer entstehen.

Eingeloggt bleiben

Ständiges An- und Abmelden kann Sie dazu verleiten, nicht mehr genau hinzusehen, auf welcher Webseite Sie sich gerade anmelden. So können Sie leichter auf Betrugsversuche hereinfallen.

Eine zweite E-Mail-Adresse oder Telefonnummer hinterlegen

So ist es dem Anbieter möglich, Ihr Konto wiederherzustellen, sollte es gehackt worden sein.

Bildschirmsperre nutzen

Das Smartphone ist Ihr persönlichstes Stück Technik und enthält viele wichtige Informationen über Sie. Sichern Sie es.

Zwei-Faktor-Authentifizierung kennenlernen

Wenn Sie sich nicht allein auf Ihr Passwort verlassen, sondern eine zweite Sicherheitskomponente wie etwa einen SMS-Code bei der Anmeldung in Ihrem Google-Konto einbinden, schützen Sie sich zusätzlich. Wer es besonders sicher haben will, verwendet einen physischen Schlüssel wie bei Googles Erweitertem Sicherheitsprogramm.

Ein gutes Passwort finden

Idealerweise ist ein Passwort schwierig zu raten und leicht zu merken. Die Anfangsbuchstaben des vorangegangenen Satzes zum Beispiel ergeben ein gutes Passwort: IiePszrulzm. Und übrigens: Es gibt keinen Grund, ein gutes Passwort, das man sich obendrein gut merken kann, regelmäßig zu ändern.

Regelmäßig den Google-Sicherheitscheck machen

In Ihrem Google-Konto können Sie unter dem Menüpunkt »Sicherheit« Schritt für Schritt Ihre Sicherheitseinstellungen in wenigen Minuten überprüfen.

Weniger preisgeben

Überlegen Sie sich gut, welche Informationen Sie im Internet öffentlich zugänglich machen. Was Sie in sozialen Medien und anderswo teilen, können unter Umständen auch Kriminelle mitlesen.

Erfahren Sie mehr zu allen Punkten auf
g.co/sicherheitscenter

Illustration: Robert Samuel Hanson

Wie erreiche ich meine Kunden online? Wie erstelle ich eine Webseite für mein Unternehmen? Wie eröffne ich einen Onlineshop? Wie werde … en? Wie funktioniert Suchmasc … eine Onlinestrategie? Wie nutze … Unternehmen? Wie funktionie … ann ich international expandieren? W … erhalten auf meiner Webseite? Wie k … en besser erreichen? Wie finden Mens … os? Wie nutze ich Videos bestn … le ich aus Daten die richtigen … t mein Unternehmensprofil in den Suche … ert Maschinelles Lernen? Wie vermeide … Onlinegeschäft? Wie kann ich agiles Arbeiten im Unternehmen einführen? Wie fördere ich unternehmerisches Denken und Handeln im Unternehmen? Wie entwickle ich neue Geschäftsmodelle? Wie kann ich mein Auftreten in Bewerbungsgesprächen verbessern? Wie schütze ich mich online? Wie kann ich produktiver arbeiten? Wie kann ich Probleme kreativ lösen? Wie spreche ich selbstbewusst über meine Erfolge?

Kostenlose Trainings zu digitalen Themen

Jetzt anmelden:
www.Zukunftswerkstatt.de

Google Zukunftswerkstatt