NR. 29 – GOO.GLE/AUFBRUCH-DE

AUFBRUCH

MENSCH UND GESELLSCHAFT IM DIGITALEN WANDEL

Cybersecurity

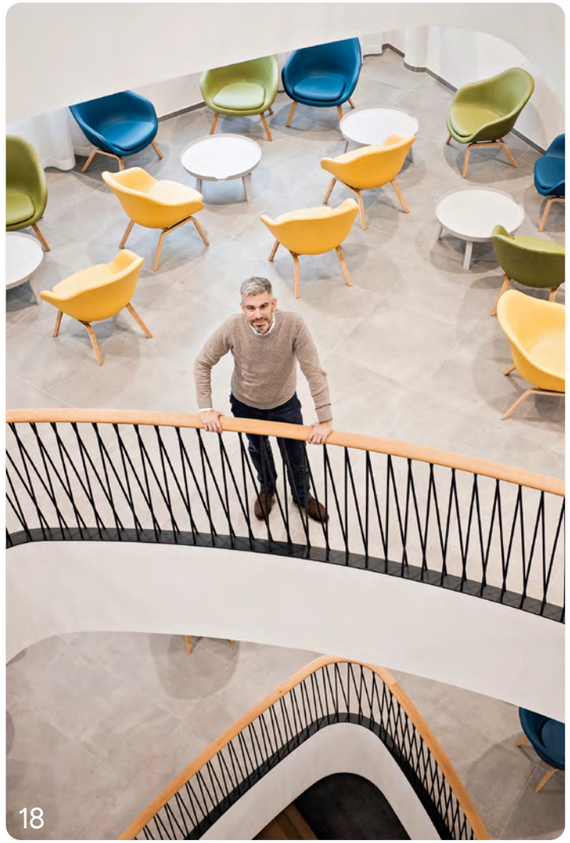
Einen Schritt voraus: Wie Unternehmen sich vor Hacker:innen schützen

Schutz von Bürgerdaten: Staatssekretär Richter über digitale Verwaltung

Exklusive Einblicke: Was Google aus einer Cyberattacke gelernt hat

Google

Inhalt



Zwei Perspektiven auf Cybersecurity: Dr. Alexander Schellong für die Schwarz Gruppe (li.) und Sabine Borsay für Google.

Cover Foto **JARED SOARES** Illustration **JOE WALDRON**

Editorial

»Wir brauchen mehr Austausch«: Unser Titelbild zeigt Sandra Joyce von der Cybersicherheitsfirma Mandiant. Ein Interview mit Joyce lesen Sie ab S. 12.

Liebe Leserin, lieber Leser,

noch nie zuvor war das Thema »Cybersicherheit« so wichtig wie heute.

Gerade vor dem Hintergrund zunehmender geopolitischer Spannungen sind Angriffe auf Informationssysteme heute zu einem festen Bestandteil von Versuchen geworden, die Volkswirtschaften und Demokratien dieser Welt zu destabilisieren.

Die Digitalisierung hat in den vergangenen Jahren enorm an Schwung gewonnen, sowohl bei Unternehmen als auch bei öffentlichen Verwaltungen und Institutionen. Wenn wir als Gesellschaft die Digitalisierung weiter vorantreiben wollen, ist es unsere gemeinsame Aufgabe, jede Einzelne und jeden Einzelnen im Netz zu schützen.

Wenn es um Cybersicherheit geht, verfügen wir bei Google über praktische Erfahrungen aus erster Hand. Unsere Systeme wehren täglich Angriffe ab. Gleichzeitig schützen wir die Sicherheit von Milliarden von Nutzerinnen und Nutzern unserer Produkte. Wir tun dies, indem wir hohe Sicherheitsstandards direkt von Anfang an in unsere Produkte einbauen, mit wichtigen Partnern auf der ganzen Welt zusammenarbeiten und auf Offenheit und Interoperabilität setzen. Weltweit entwickeln Kolleginnen und Kollegen Produkte, die die Menschen, Unternehmen und Organisationen im Netz noch besser schützen – auch hier in Deutschland, in unserem Google Safety Engineering Center in München.

Cybersicherheit ist in der heutigen mobilen, hybriden Umgebung eine Gemeinschaftsaufgabe. Sie erfordert die enge Zusammenarbeit von Politik, Forschung und Wirtschaft, über Ländergrenzen hinweg. Wie das funktionieren kann, stellen wir Ihnen in dieser Ausgabe des *Aufbruch*-Magazins anhand von Beispielen und Projekten konkret und anschaulich vor.

Viel Spaß beim Lesen!

Ihr Philipp Justus
Vice President Google Zentraleuropa

Fotos **EMANUEL HERM, FLORIAN GENEROTZKY, GOOGLE LLC** Illustration **CAMILO HUINCA**

Gehackt!

Privatleute, Unternehmen, Staat und Verwaltung sind im Internet so vielen Datendiebstählen und Hackerangriffen ausgesetzt wie nie zuvor. Sicherheit im Netz spielt für alle Bereiche der Gesellschaft eine wichtige Rolle. Jede und jeder ist dabei selbst in der Verantwortung, sich zu schützen – und damit die Cybersicherheit für alle zu erhöhen.

Cybersecurity

Mit **Cybersecurity** oder auch IT-Sicherheit sind alle Maßnahmen gemeint, um böswillige Hackerangriffe auf Computer, mobile Geräte, Server, elektronische Geräte, Netzwerke und Daten abzuwehren.

Ransomware-Angriff

50 000 000

US-Dollar forderten Hacker:innen 2021 von Acer nach einem **Ransomware-Angriff.**

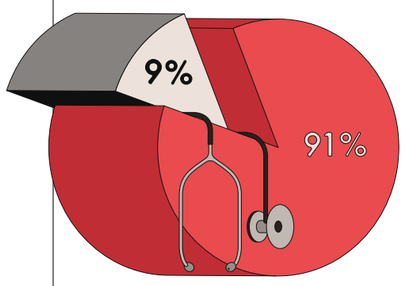
Datenleck

Von einem **Datenleck** oder einer Datenpanne wird dann gesprochen, wenn sich Unbefugte Zugang zu einem Unternehmensnetzwerk oder einer Datensammlung verschaffen.

Social Engineering

Bei etwa 48 Prozent der deutschen Unternehmen gab es laut einer Bitkom-Studie in den vergangenen zwei Jahren Versuche von **Social Engineering.** Dabei erschleichen Hacker:innen sich am Telefon oder per E-Mail das Vertrauen von Mitarbeiter:innen in Unternehmen und bringen diese dazu, sensible Daten preiszugeben oder interne Sicherheitsvorkehrungen zu umgehen und den Angreifer:innen so Zutritt zum Unternehmensnetzwerk zu verschaffen.

Datenschutzvorfall



91 Prozent der Gesundheitseinrichtungen hierzulande waren laut einer Studie des IT-Dienstleisters SOTI seit 2020 von einem **Datenschutzvorfall** betroffen.

Malware

Malware (Überbegriff für Schadsoftware) nutzen Hacker:innen, um die Sicherheitsvorkehrungen von Computern, Mobilgeräten, Netzwerksystemen zu umgehen: Sie kann Daten löschen, verschlüsseln, manipulieren, sammeln oder die Kontrolle über Systemfunktionen übernehmen. Der gehackte Rechner kann andere Computer als Teil eines Botnetzes angreifen.

Text **CHRISTIANE MANOW-LE RUYET**

Cyberkriminalität

146 363

Fälle von **Cyberkriminalität** zählte das Bundeskriminalamt 2021 in Deutschland – Tendenz weiter steigend.

Ransomware (Erpressungssoftware)

Ransomware ist eine spezielle Form von Malware und stellt im Internet die größte Bedrohung für Unternehmen und Einzelpersonen dar. Sie kann Daten eines Computers verschlüsseln und unbrauchbar machen. Ganze Produktionsstraßen können so stillgelegt werden. Kriminelle verlangen meist ein Lösegeld (englisch: ransom), um die Daten zu entschlüsseln und damit die Systeme wieder zum Laufen zu bringen.

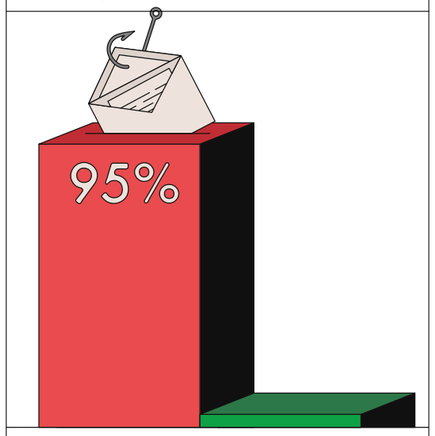
Doxing

Doxing wird auch im Zusammenhang mit Hacking erwähnt. Darunter versteht man das Zusammentragen und Veröffentlichen persönlicher Daten wie Adressen, Telefonnummern oder Bankverbindungen. Ziel ist es, die Opfer einzuschüchtern. Seit 2021 drohen Täter:innen hierfür bis zu drei Jahre Haft.

Passwörter

»123456« gehört zu den beliebtesten, aber auch unsichersten **Passwörtern** – für Hacker:innen die größten Einfallstore für Cyberkriminalität. Ein Passwortmanager hilft, unsichere Passwörter zu vermeiden.

Phishing



95 Prozent der IT-Sicherheitsvorfälle entstehen laut einem Bericht des Weltwirtschaftsforums durch menschliche Unachtsamkeit: Wenn etwa **Phishing-**Links unachtsam geöffnet werden, kann sich Schadsoftware schnell verbreiten. Auch wenn sich Hacker:innen als Kolleg:innen ausgeben und nach Zugangsdaten fragen, können Daten ausgespäht werden.

Illustrationen **CAMILO HUINCA**

Operation Aurora

oder: Wie sicher ist das Internet?

Die Angreifer:innen sind unsichtbar, die Schäden, die sie anrichten, immens. Immer raffinierter gehen Cyberkriminelle vor, um an sensible Daten zu gelangen, häufig mit dem Rückhalt staatlicher Akteure. Ein Hackerangriff 2009 auf Google legte offen, wie verwundbar Netzwerke sind – und führte dazu, dass Internet-Nutzer:innen heute so sicher sind wie nie zuvor

Heather Adkins erinnert sich nur zu gut an den 14. Dezember 2009, einen Montag. Gegen 16 Uhr kehrte die Sicherheitsexpertin aus einer Besprechung in der Google-Zentrale im kalifornischen Mountain View an ihren Schreibtisch zurück. Eine Gruppe von Mitarbeiterinnen und Mitarbeitern hatte sich um einen Computer geschart und berichtete, sie hätte »sehr interessante« Aktivitäten im Unternehmensnetzwerk festgestellt. Eine harmlose Umschreibung für eine überaus ernste Situation: Hacker:innen hatten sich Zugriff zu einem Server im Rechenzentrum verschafft – einem von Tausenden Geräten im Firmennetzwerk.

Adkins schwante, dass es nicht dabei bleiben sollte. »Das war kein normales Ereignis«, erzählt die Managerin, die heute für die weltweite Sicherheitstechnik bei Google verantwortlich ist. Am folgenden Tag waren bereits mehrere Rechner betroffen. »Die Geschwindigkeit und die Anpassungsfähigkeit der Angreifer:innen waren außergewöhnlich.«

Ein Angriff lief an, der als »Operation Aurora« in die Geschichte des Datenschutzes eingehen sollte – und Google dazu veranlasste, die eigenen Sicherheitsstrukturen umfassend umzubauen und zu erweitern. Die wichtigste Lektion: Wer Bedrohungen effektiv bekämpfen will, muss das Internet so betrachten, wie es die Hacker:innen tun.

Ein scheinbar harmloser Link

In diesem Fall war das Vorgehen der Angreifer:innen so simpel wie wirkungsvoll: Sie hatten eine scheinbar harmlose E-Mail an einen Google-Mitarbeiter geschickt mit einem ebenso harmlos wirkenden Link. Der Mitarbeiter klickte diesen Link an, so wie es weltweit rund fünf Milliarden Mal am Tag geschieht. Doch diesmal öffnete sich keine Datei mit Firmenzahlen, Testergebnissen oder einem Katzenvideo. Stattdessen lud eine Schadsoftware auf den Rechner des Mitarbeiters herunter; die Hacker:innen hatten Zugang zum kompletten Google-Netzwerk.

»Wir hatten kein Drehbuch für so eine Situation«, erinnert sich der damalige Sicherheitschef Eric Grosse. »Wir haben alles fallen lassen und uns nur noch hierauf konzentriert.« Anfangs belegte das Team, das sich um die Aufklärung des Angriffs kümmern sollte, einen Konferenzraum. Schnell waren es drei, dann vier Räume – schließlich ein ganzes Gebäude. Aus aller Welt wählten sich Spezialist:innen in Telefonkonferenzen ein, andere wurden in die Firmenzentrale nach Mountain View eingeflogen.

Heather Adkins drückte ihnen Listen mit den betroffenen Rechnern in die Hand und sagte: »Los, schnappt sie euch!« Und so fing das Team an, mitten in der Nacht die Festplatten betroffener Computer auf dem Campus auszubauen, um sie eingehend zu untersuchen. Doch das dauerte zu lange. Also griffen sie sich bald die kompletten Rechner und hinterließen auf dem Schreibtisch eine Notiz für die Besitzerinnen und Besitzer.

Derweil griff Adkins zum Telefon und besprach sich mit anderen Fachleuten in der Branche. Einer davon war Dmitri Alperowitsch, der damals für McAfee arbeitete, einen Hersteller von Computersicherheitssoftware. Gemeinsam mit einigen Mitarbeiterinnen und Mitarbeitern unterstützte er sofort das Google-Team bei dessen Analyse. Im Code der Schadsoftware entdeckte er ein Wort, das der Operation ihren Namen gab: Aurora. So hieß der russische Panzerkreuzer, der 1917 in Sankt Petersburg einen Schuss abgab und so die Oktoberrevolution in Gang setzte.

Immer einen Zug voraus

Operation Aurora war ein Schlüsselerlebnis – mit weitreichenden Folgen für Google und das gesamte Internet. »Wir mussten unseren Ansatz in der Cybersicherheit komplett verändern, um der neuen Bedrohung zu begegnen«, sagt Alperowitsch.

Zunächst ging es jedoch darum, die Angreifer:innen einzukreisen – und vom Netzwerk zu trennen. Kurz vor Weihnachten, knapp zehn Tage nach der Attacke, war es so weit. Es folgte der größte Eingriff in die internen Systeme seit Googles Gründung: Sämtliche Mitarbeiterinnen und Mitarbeiter wurden binnen einer Stunde aus dem Firmennetzwerk geworfen. So sollte auch die letzte Verbindung der Hacker:innen gekappt werden. Wenig später stand fest: Die Aktion war erfolgreich, die Angreifer:innen wurden aus dem Netzwerk verbannt, und Systeme und Zugriffe der Mitarbeiterinnen und Mitarbeiter konnten wiederhergestellt werden.

Die wichtigste Frage blieb jedoch unbeantwortet: Wer steckte hinter dem Angriff?

Nur wenige Wochen später, am 12. Januar 2010, gab Google bekannt, gehackt worden zu sein. Es stellte sich heraus, dass mindestens 20 weitere Technologiekonzerne betroffen waren, und alle Spuren führten nach China. Bei Google wollten die Hacker:innen offenbar an Gmail-Konten von Aktivist:innen gelangen, die sich für Menschenrechte in China einsetzten. Nach internen Untersuchungen wurde dieses Ziel aber nicht erreicht.

Operation Aurora löste seismische Veränderungen in Googles Sicherheitsstrategie aus: Technologien, Netzwerkarchitektur, Branchenstandards – alles wurde infrage gestellt. Am wichtigsten jedoch: Fortan kümmerten sich hoch spezialisierte Teams um die Gefahren, die von Hacker:innen ausgehen. Eines der neuen Teams, die damals als Reaktion auf den Angriff gegründet wurden, war die »Threat Analysis Group« – kurz TAG. »Unser wichtigster Job ist zu verstehen, wie die Angreifer:innen vorgehen, um sie zu stoppen und unsere Nutzerinnen und Nutzer vor ihnen zu schützen«, sagt Shane Huntley, der das Team leitet.

TAG beobachtet mittlerweile mehr als 270 Akteure, die auf Geheiß von Regierungen im Internet Angriffe verüben, sich bereichern oder Desinformation streuen. Und verfolgt Attacken anhand der Schadsoftware zurück, die dabei zum Einsatz kommt.

Die Expert:innen setzen dabei auf eine Technologie, die auch in der Google Suche zum Einsatz kommt. Sie geben Ausschnitte des Codes von Schadprogrammen ein, und die Such-Software ermittelt dann, woher sie stammen. So fanden sie beispielsweise heraus, wer hinter dem »WannaCry«-Angriff 2017 steckte, bei dem an einem Tag weltweit über 200 000 Computer in Unternehmen, Universitäten, ja sogar im britischen Gesundheitssystem lahmgelegt wurden: die Regierung in Nordkorea. Die Schadsoftware verschlüsselte nach Befall eines Computers bestimmte Benutzerdateien. Die Absender forderten die Nutzerinnen und Nutzer auf, ein Lösegeld in Bitcoin zu zahlen – andernfalls würden die Daten gelöscht. Der Schaden wird auf mehrere Hundert Millionen bis zu einigen Milliarden US-Dollar geschätzt. Europol erklärte damals, dass es sich um einen Angriff nie dagewesenen Ausmaßes handele.

1,5

Millionen **Cyberattacken** ereigneten sich 2021 in Deutschland – Dunkelziffer inklusive. Das entspricht rund **4000** Attacken am Tag.

Text **CHRISTIAN BAULIG**

Die Erkenntnisse aus den Angriffen helfen Google dabei, Produkte sicherer zu machen: Davon profitieren unter anderem mehr als eine Milliarde Nutzerinnen und Nutzer des E-Mail-Dienstes Gmail. So filtert Google dank der Erkenntnisse von Teams wie TAG über 99,9 Prozent aller unerwünschten Mails heraus, mit denen Kriminelle Nutzerinnen und Nutzer dazu bringen wollen, Schadsoftware herunterzuladen oder sensible Informationen preiszugeben.

Eine digitale Feuerwehr

Doch die Angreifer:innen werden immer cleverer, ihre Methoden immer dreister: So versuchten Hacker:innen 2021, sich direkten Zugang zu Googles Sicherheitsexpert:innen zu verschaffen, indem sie sich als vermeintliche Kolleginnen und Kollegen tarnten: Passende Social-Media-Konten, Websites, Blogs – an alles hatten die Hacker:innen gedacht, um Vertrauen zu schaffen. »So wollten sie Zugriff auf unsere Rechner bekommen«, erzählt Heather Adkins.

Wie sich herausstellte, ließ sich ein Google-Mitarbeiter tatsächlich in eine Unterhaltung verwickeln. Sofort untersuchten Expertinnen und Experten gründlich den Rechner: Mit wem kommuniziert die Schadsoftware? Welche Domainnamen und IP-Adressen tauchen auf? Wie breitet sich die Software auf dem Rechner aus? Die Spuren führten – wieder nach Nordkorea.

Doch war dies der einzige betroffene Rechner? Um diese Frage zu beantworten, trat Googles »Detection and Response«-Team auf den Plan, eine Art digitale Feuerwehr. Mithilfe spezieller Software können die Spezialist:innen in kürzester Zeit gewaltige Datenmengen analysieren und feststellen, ob bestimmte Muster auf einem kompromittierten Computer oder Server auch bei anderen Geräten erkennbar sind. Ist das der Fall, schaut sich ein Spezialist oder eine Spezialistin den Computer genauer an. Wie bei Operation Aurora gelang es auch diesmal, die Angreifer:innen zu isolieren und von den betroffenen Rechnern abzuschneiden. Nur zwei Rechner waren betroffen, niemand erlitt einen Schaden. Mission geglückt!

Hacker:innen im eigenen Unternehmen

Google beschränkt sich nicht darauf, auf Angriffe von außen zu reagieren. Das Unternehmen beschäftigt selbst Hacker:innen, die tagein, tagaus die eigenen Sicherheitsmechanismen auf die Probe stellen: das sogenannte Offensive Security Team – auch »Red Team« genannt.

»Das Red Team ist mein Lieblingsgegner«, sagt Heather Adkins, »es eröffnet uns eine völlig →

Hacking Google

Eine sechsteilige YouTube-Serie erzählt die Geschichte rund um den großen Hacker-Angriff auf Google – die Operation Aurora.
goo.gle/hackinggoogle-serie

Illustrationen **JOE WALDRON**

Heather Adkins leitete das Team, das den größten Hackerangriff in der Geschichte von Google stoppte.

neue Sicht auf das System.« Als vor zehn Jahren die Datenbrille Google Glass entwickelt wurde, versuchten die hauseigenen Hacker:innen, an Designdokumente und andere vertrauliche Informationen heranzukommen. Ihr Trick: Sie schickten Mitarbeiter:innen, die gerade Betriebsjubiläum hatten, ein vermeintliches Firmengeschenk – eine kleine Plasmalampe, die über einen USB-Anschluss mit Strom versorgt wird. Sobald die Lampe mit dem Rechner verbunden war, installierte sich fast unmerklich und automatisch eine Software, die es dem Red Team erlaubte, E-Mails im Namen des Mitarbeiters oder der Mitarbeiterin zu verschicken. Die Hacker:innen arbeiteten sich immer weiter vor – bis zu den gesuchten Dokumenten. Die Sache flog erst auf, als ein Mitglied des Red Teams im Namen einer berechtigten Person eine Muster-Brille abholen wollte.

Die Erkenntnis für Googles Sicherheitsexpert:innen: Selbst in einem überdurchschnittlich gut abgesicherten Tech-Unternehmen ist es möglich, in die Systeme einzudringen und an vertrauliche Informationen zu gelangen. Als Konsequenz wurde die USB-Schnittstelle, die hunderttausendfach in die Hardware eingebaut ist, gegen das Eindringen von Schadsoftware abgesichert. So werden unter anderem verdächtige Datentransporte sofort abgebrochen. Auch das Speichern von Daten auf USB-Sticks ist heute standardmäßig ausgeschaltet.

Belohnung für Software- und Hardware-Fehler

Prävention ist wichtig. Deshalb bedient sich Google der Intelligenz derer, die Google-Produkte nutzen. »Wir suchen ständig nach Fehlern in unseren Programmen, aber es gibt Dinge, die wir übersehen«, sagt Eduardo Vela Nava, Cheftechniker in Googles »Bug Hunters Program«. Dieses Programm belohnt diejenigen, die Fehler und damit potenzielle Sicherheitslücken in Google-Produkten melden. Die Zahl der Meldungen steigt Jahr für Jahr, nicht zuletzt, weil das Unternehmen immer höhere Beträge für »Bug Reports« auslobt. Dieser Anreiz motiviert alle, Schwachstellen zu erforschen, zu melden und zu beseitigen – und kommt am Ende Menschen weltweit zugute.

Google hat dabei nicht nur die eigenen Systeme und Produkte im Blick, sondern das gesamte Internet.

Im Fokus der Spezialist:innen stehen sogenannte Zero-day Vulnerabilities, also unentdeckte Schwachstellen, die Unternehmen im Fall eines Angriffs null Tage Zeit lassen, die Schwachstelle zu beheben. »Manchmal ist der schwächste Punkt bei Google ein Produkt, das gar nicht von Google stammt«, sagt Tim Willis aus Googles »Project Zero Team«. Einfallstor bei der Operation Aurora war zum Beispiel eine Schwachstelle im Microsoft-Browser Internet Explorer. Die Angreifer:innen platzierten darüber eine Schadsoftware, die ihnen Zugriff auf das System gab.

Bis heute hat das Team von Project Zero, das 2014 gegründet wurde, mehr als 1800 solcher Schwachstellen aufgedeckt. Die Sicherheitsingenieur:innen prüfen zum Beispiel Betriebssysteme, Browser oder Open-Source-Software auf mögliche Angriffsstellen. Ihr Ziel ist es, diese zu beseitigen, um das Netz für alle Nutzerinnen und Nutzer sicherer zu machen.

Je schneller, desto besser

Denn Menschen nutzen eine Fülle unterschiedlicher Geräte und Programme, die alle miteinander vernetzt sind. Und Schwächen in einem Teil des Systems bedrohen alle Teile des Systems.

Das Team fordert deshalb technische Geräte und Softwaredienste und -systeme aller möglichen Hersteller heraus. So brachten Google-Hacker:innen Handys dazu, Bilder und Ton zu übertragen, ohne dass die Besitzer:innen dies bemerkten. Fünf verschiedene Videochat-Programme waren betroffen. Google informierte die Hersteller – und in kurzer Zeit wurden die Lücken geschlossen.

Die Realität ist, dass dieses spezialisierte Sicherheitsteam ähnliche Schwachstellen wie nationalstaatliche und kriminelle Angreifer findet, weshalb es wichtig ist, dass diese Probleme schnell behoben werden, sobald sie entdeckt werden. Leider schaffen nicht alle Unternehmen diese Probleme schnell aus der Welt. »Es war ziemlich üblich für bestimmte Unternehmen, dass sie mehr als sechs Monate benötigten, um einen Fehler zu beseitigen, wenn man ihnen einen meldete«, sagt Willis, »und einige von ihnen wurden nie behoben.« Heute haben die betroffenen Unternehmen 90 Tage Zeit, um den Fehler zu korrigieren. Andernfalls macht Google die Schwachstelle öffentlich – was für Unternehmen eine starke Motivation ist, ihre Schwachstellen schnell zu beheben.

Dass Kundendaten sicher sind, Dienste ständig verfügbar und Nutzerinnen und Nutzer vor Angriffen geschützt, ist für Unternehmen existenziell. Intensives Training, ständiges Infragestellen und schnelles Handeln sorgen dafür, dass es für Hacker:innen immer schwieriger wird, an ihr Ziel zu gelangen. Viele Risiken für Internetnutzer:innen konnten in den vergangenen Jahren ausgeschlossen werden. Bei alledem sollte man sich jedoch nicht in falscher Sicherheit wiegen. Denkt Heather Adkins an Operation Aurora zurück, tut sie dies mit einer Mischung aus Stolz und Demut. »Wir haben sie gestoppt«, sagt sie, »aber ich bin nicht davon überzeugt, dass sie es nicht noch einmal versuchen könnten.«

Die häufigsten Bedrohungen

Gesellschaft
- Identitätsdiebstahl
- Sextortion
- Fake-Shops im Internet

Wirtschaft
- Ransomware
- IT-Supply-Chain-Angriffe
- Schwachstellen
- offene oder falsch konfigurierte Online-Server

Regierung & Verwaltung
- Ransomware
- Angriffe auf kritische IT-Infrastruktur
- Schwachstellen
- offene oder falsch konfigurierte Online-Server

Foto **CAYCE CLIFFORD**

Das Ausmaß von Cyberkriminalität hat massiv zugenommen, sagt Sandra Joyce von Mandiant.

»Wir brauchen mehr Austausch«

Interview **CHRISTIAN HEINRICH**

→ Frau Joyce, Sie arbeiten seit vielen Jahren in der Cybersicherheit. Wie haben sich Cyberattacken in den letzten Jahren verändert – und womit dürften wir künftig noch konfrontiert werden?
Ich erinnere mich an einen Vortrag, den ich vor fünf Jahren in Frankreich gehalten habe. Als ich damals sagte, dass einige Hacker:innen 300 000 Euro Lösegeld forderten, war jeder im Publikum schockiert. Heute sind Lösegeldforderungen von zehn Millionen US-Dollar und mehr ziemlich normal. Das ist nur ein Beispiel, das zeigt: Ausmaß und Häufigkeit von Cyberkriminalität haben in den letzten Jahren dramatisch zugenommen.

Wie haben sich dagegen die Fähigkeiten im Bereich Cybersicherheit entwickelt?
Die haben sich in der letzten Zeit sehr verbessert. Zusammen mit der Demokratisierung von Information sehen wir jetzt auch eine Demokratisierung von Cybersicherheit. Sogar kleinere Staaten haben die Fähigkeit, etwas beim Thema Cybersicherheit zu bewirken. Und auch die Public-Cloud-Technologie demokratisiert die Sicherheit.

Mandiant unterstützt Firmen auf der ganzen Welt dabei, sich gegen Cyberattacken zu schützen. Wie lautet Ihr wichtigster Rat an Unternehmen?
Ransomware ist momentan das dringendste Problem. Etwas, auf das man sich vorbereiten muss. Als Unternehmen sollten Sie mit Ihren Entscheidern Trainings durchführen und proben, wie Sie im Falle einer Ransomware-Attacke vorgehen. Sonst kann Sie ein tatsächlicher Angriff eiskalt erwischen. Unternehmen sollten zudem prüfen, wie gut sie ihre Netzwerke segmentiert haben. Die Kronjuwelen …

… sensible Daten und Informationen …
… sollten isoliert werden von den Netzwerken, in denen die tägliche Arbeit erledigt wird. Und schließlich sollten Sie als Unternehmen in der Lage sein zu erkennen, wenn ein Einbruch in Ihr IT-System stattfindet. Wenn das nicht der Fall ist, sorgen Sie dafür, dass diese Kompetenz in Ihrem Unternehmen vorhanden ist. Denn die meisten Angreifer:innen werden erst nach einiger Zeit aktiv, je nachdem, welche Ziele sie verfolgen. Wenn sie Ransomware einschleusen wollen, agieren sie so schnell wie möglich, aber auch das kann immer noch mehrere Stunden oder Tage dauern. Wenn die Angreifer:innen darauf aus sind, Informationen zu erhalten und Spionage zu betreiben – sie etwa im Auftrag von Regierungen agieren –, bleiben sie jahrelang im Netzwerk und beobachten und sammeln Daten.

Wie genau unterstützt Mandiant Unternehmen gegen Cyberattacken?
Wir arbeiten in zwei großen Bereichen: Incident Response und Threat Intelligence. Wenn ein Unternehmen von einem Sicherheitsvorfall betroffen ist, kann es sich an uns wenden. Dann unterstützen wir es dabei, die Angreifer:innen im Netzwerk aufzuspüren und die Lage zu entschärfen, und wir machen Vorschläge, wie das Netzwerk neu aufgesetzt und die Situation geklärt werden kann. Unsere andere Kernkompetenz ist proaktiver: Wir suchen im Internet ständig nach verdächtigen Aktivitäten von Angreifer:innen. Wir beobachten das Deep- und das Darknet, wo sich Hacker:innen austauschen. Wenn diese beispielsweise Daten anbieten, die sie erbeutet haben, warnen wir die betroffenen Unternehmen, dass sie ein Sicherheitsproblem haben – manchmal sogar, bevor sie das Problem überhaupt bemerken.

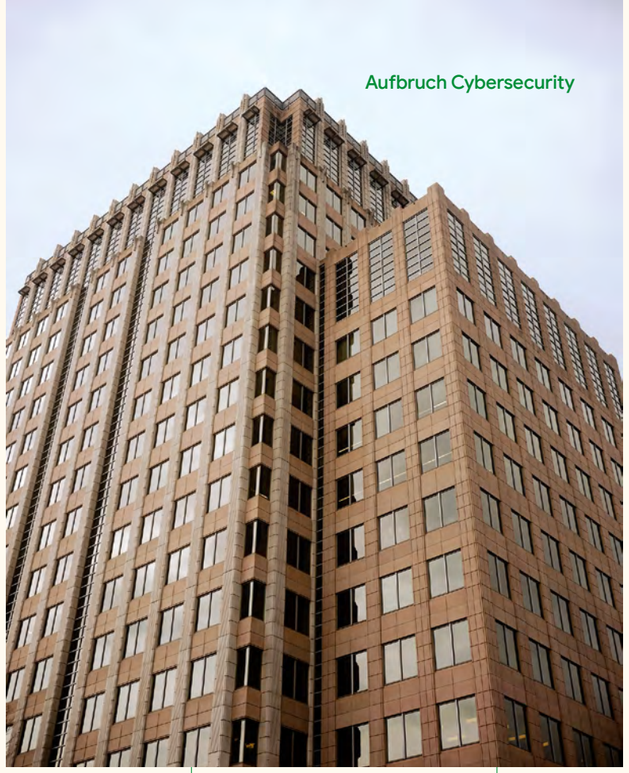
Hacker:innen zur Verantwortung zu ziehen stellt eine enorme Herausforderung dar. Doch Unternehmen können sich besser vor ihnen schützen, sagt Sandra Joyce, Vizepräsidentin von Mandiant Intelligence, ein auf Cybersicherheit spezialisiertes Unternehmen, das jetzt zu Google gehört

Wie gelangen Sie in diese Darknet-Foren?
Wir sind dort notwendigerweise unter falscher Identität unterwegs und lesen mit, wenn Hacker:innen sich austauschen.

2022 hat Google Cloud Mandiant übernommen. Was bringt Mandiant mit zu Google und den Kunden von Google Cloud?
Wir sind immer noch ziemlich neu bei Google, aber wir sind schon dabei, mithilfe unserer Erkenntnisse Einzelpersonen über Bedrohungen zu informieren, Googles eigene Cyberabwehr zu stärken und die Sicherheitsprodukte für Google Cloud und seine Kunden zu erweitern. Mit unserem Wissen →

Zur Person

Sandra Joyce ist Vizepräsidentin von Mandiant Intelligence bei Google Cloud. Das auf IT-Sicherheit spezialisierte Unternehmen wurde 2022 von Google übernommen.



können wir einen wichtigen Beitrag leisten, denn wir kennen Bedrohungen aus der ganzen Welt, nicht nur aus der Google-Umgebung.

Inwieweit verändert die gegenwärtige politische Lage die Cybersicherheit?
Der Angriffskrieg Russlands gegen die Ukraine etwa hat die Cyberabwehr anfangs in erhöhte Alarmbereitschaft versetzt. Es besteht die Gefahr russischer Cyberaggression über das ukrainische Kampfgebiet hinaus. So gab es bereits einige Angriffe auf die Internetseiten von US-Flughäfen, die von Hacktivist:innen mit Verbindungen zur russischen Regierung verübt wurden. Aber die Auswirkungen in diesen und anderen Fällen waren bis heute minimal. Hacker:innen versuchen auch, falsche Informationen zu streuen; russische Hacktivist:innen konzentrieren sich darauf, einen Keil zwischen die Ukraine und ihre Verbündeten zu treiben.

Wie steht es um die »Big Four« im Cyberraum, Russland, Iran, China und Nordkorea? Was können wir in Zukunft von ihnen erwarten?
Alle vier sind relevant und zurzeit sehr aktiv. Russland ist dieser Tage ziemlich selbsterklärend mit seinem Vorgehen in der Ukraine. Nordkorea nutzt Kryptowährungsbörsen und Infrastrukturen für Kryptomining aus, um die Aktivitäten der Regierung zu finanzieren. Iran ist allgemein sehr agil, wir beobachten hier eine ständige Aktivität und haben mit dem Iran verbundene Akteure entdeckt, die Länder wie Albanien im Visier haben. Und wir sehen, dass China wieder viel Spionage und Diebstahl von geistigem Eigentum betreibt.

Wie schätzen Sie die gegenwärtige Situation im Bereich Cybersicherheit in Deutschland ein?
Wie viele Länder erfährt Deutschland gerade eine zunehmende Anzahl von Ransomware-Angriffen. Auf den Seiten, auf denen gestohlene Daten getauscht werden, zählen wir regelmäßig die Betroffenen nach Ländern. In Deutschland hat sich ihre Zahl seit 2020 verdoppelt. Die Länder, die im Bereich Cybersecurity äußerst erfolgreich sind, haben sehr enge Verbindungen zum privaten Sektor – national und international. Weil Cybersicherheit ein »Mannschaftssport« ist, kann man sie nicht alleine bewerkstelligen. Deutschland ist auf dem Weg dahin.

Das Cybersecurity-Unternehmen Mandiant hat seinen Sitz in der Stadt Reston im US-Bundesstaat Virginia.

In vielen Fällen werden Hacker:innen für ihre Angriffe nicht zur Verantwortung gezogen. Sehen Sie eine Möglichkeit, das zu ändern?
Viele der Cyberkriminellen sitzen in Ländern, in denen sie weder von Europol noch von US-Behörden verfolgt werden können. Wenn sie beispielsweise von irgendwo in Russland aus agieren, können sie weiter hacken, ohne bestraft zu werden. Daher wird Cyberkriminalität weiterhin nur mit einem geringen Risiko verbunden sein – was verlockend ist. Auch das ist ein Grund, warum sie uns so lange erhalten bleiben wird, bis sich die Beziehungen zwischen Regierungen verbessern und diplomatische Lösungen gefunden werden.

Und wie sollte man dieser Herausforderung begegnen?
Angreifer:innen sind am erfolgreichsten, wenn ihre Opfer nicht miteinander reden. Wir müssen viel offener Informationen über Sicherheitsverletzungen und Bedrohungen austauschen. Und: Das Internet wurde in seinen Anfängen entwickelt, ohne den Sicherheitsaspekt zu berücksichtigen. Aber wenn wir künftig Neues in das Internet integrieren, sollten Sicherheitsüberlegungen und -konzepte von Beginn an mit eingebunden werden.

Fotos **JARED SOARES**

Angebote für mehr Sicherheit

Viele Gruppen sind besonderen Gefahren im Internet ausgesetzt, dazu gehören Unternehmerinnen und Unternehmer, Menschen in der Politik oder Medienschaffende. Mit speziellen Angeboten unterstützt Google diese Organisationen und Personen dabei, sich effektiv vor Cyberattacken zu schützen

⟶ Es passiert tausendfach in deutschen Unternehmen: Unbekannte verschaffen sich Zugang zum Computer einer Mitarbeiterin oder eines Mitarbeiters und installieren Schadsoftware (Malware). Jetzt stehen alle Tore offen: Die Schadsoftware zeichnet Tastenanschläge auf, um die Details von Passwörtern zu erfassen, oder stiehlt auf dem Rechner gespeicherte Sicherheitsschlüssel, die zur Authentifizierung nötig sind. Das Szenario, das in den Sicherheitstrainings der Google Zukunftswerkstatt vorgestellt wird, ist der Albtraum für Unternehmerinnen und Unternehmer. Haben sich Hacker:innen in den IT-Systemen festgesetzt, werden oft wichtige Daten blockiert oder gestohlen. Es droht der Stillstand der Firma.

»Für Firmen ohne große IT-Abteilung ist Cybersicherheit eine gewaltige Herausforderung«, sagt Verena Gauthier, die neben Lena Rohou die Google Zukunftswerkstatt in Deutschland verantwortet. Seit 2014 unterstützt die Initiative von Google Menschen dabei, ihre Digitalkompetenzen auszubauen, und hilft Unternehmen, ihre Wettbewerbsfähigkeit für die Zukunft zu sichern. Wie groß die Herausforderung der Cybersicherheit ist, zeigt eine Umfrage, die das Marktforschungsunternehmen Kantar 2022 im Auftrag von Google unter 250 kleinen und mittleren Unternehmen in Deutschland durchgeführt hat: Vier von zehn Firmen wurden demnach in den zurückliegenden zwei Jahren Opfer einer Attacke aus dem Internet. Nur zwölf Prozent der Befragten gaben an, auf einen Cyberangriff »sehr gut vorbereitet« zu sein.

Sicherheitskultur schaffen

Um diese Lücke zu schließen, bietet Google seit Kurzem spezielle Kurse zu den Themen Cybersecurity und Datenschutz an. Hier lernen Unternehmerinnen und Unternehmer anhand von Beispielen unter anderem, wie Firmendaten in der Cloud gesichert werden. Und es geht darum, wie Unternehmen eine Sicherheitskultur schaffen, die digitale Angriffe verhindert.

In Kursen der Google Zukunftswerkstatt können Menschen ihre Digitalkompetenzen ausbauen.

Foto **FELIX BRÜGGEMANN**

Eine Übersicht über die kostenlosen Online-Trainings, für die kein Vorwissen nötig ist, gibt es im Netz unter ***zukunftswerkstatt.de***

Die Workshops für KMUs ordnen sich ein in eine Reihe von Angeboten, mit denen Google speziellen Zielgruppen Kenntnisse vermittelt, wie sie sich besser schützen.

Eine wichtige Rolle dabei spielt das erweiterte Sicherheitsprogramm von Google, das ebenfalls kostenlos angeboten wird: Es ist der stärkste Kontoschutz von Google und schützt vor gezielten Online-Angriffen. Allgemein dient das Programm dazu, unbefugten Kontozugriff zu verhindern, da für die Anmeldung ein physischer Sicherheitsschlüssel erforderlich ist. Darüber hinaus bietet das Programm zusätzlichen Schutz vor schädlichen Downloads. Downloads werden zusätzlichen Prüfungen unterzogen. Wenn eine Datei heruntergeladen wird, die möglicherweise schädlich ist, werden Nutzerinnen und Nutzer benachrichtigt oder der Download wird blockiert. Außerdem wird der Zugriff auf Google-Kontodaten auf Google-Apps und geprüfte Drittanbieter-Apps reduziert.

Sicherer im Internet!

Digitale Sicherheit verständlich machen

»Viele Eltern wollen, dass ihr Kind im Umgang mit Medien auch digitale Kompetenzen erlernt, um sicher im Netz unterwegs zu sein. Kinder- und Familiensicherheit ist daher ein zentrales Thema für Google. Im GSEC in München sprechen wir mit Kindern und Jugendlichen, um digitale Sicherheit und Privatsphäre-Einstellungen noch einfacher und noch verständlicher zu machen. So haben wir etwa Datenschutzinformationen für Jugendliche entwickelt, die sich speziell an 13- bis 17-Jährige richten, die sich über den Umgang mit Daten bei Google informieren wollen. Zudem setzen wir Richtlinien auf, die speziell jüngere Nutzerinnen und Nutzer schützen, und stellen leicht zu verstehende Informationsmaterialien bereit. Kürzlich haben wir etwa das Sicherheitscenter für Familien ins Leben gerufen, das Tipps für den Umgang mit Medien bietet und dabei hilft, digitale Grundregeln zu etablieren.«

Anja Dinhopl, Research-Managerin im Forschungszentrum für Kinder- und Online-Sicherheit ⟶ ***safety.google/families***

Passwörter sicher verwalten

»Der Google Passwortmanager hilft, sicherere, sich nicht wiederholende Passwörter für Onlinekonten zu erstellen, einzutragen und zu verwalten. Er sorgt dafür, dass Passwörter geräteübergreifend zur Verfügung stehen und eine einfache, sichere Anmeldung ermöglichen. Er schützt auch zuverlässig vor Phishing-Angriffen. Webseiten, die andere Seiten imitieren, um deren Passwörter abzugreifen, werden nicht mit Passwörtern gefüllt. Sollten durch Sicherheitslecks auf anderen Webseiten Anmeldedaten der Nutzer:innen kompromittiert und veröffentlicht werden, informiert Google die Nutzer:innen, damit sie ihre Anmeldedaten ändern können. Inzwischen kann man sich auch mit Passkeys im Internet anmelden. Diese Verschlüsselungselemente muss man sich nicht merken, und sie können auch nicht gestohlen werden. Passkeys werden auf den Geräten gespeichert, Nutzer:innen bestätigen ihre Anmeldungen mit der Displaysperre, etwa dem Fingerabdruck. Passkeys lassen sich wie gewohnt im Passwortmanager verwalten.«

Andreas Türk, Produktmanager für den Google Passwortmanager ⟶ ***passwords.google.com***

Text **CHRISTIAN BAULIG**

Das Handeln der Menschen ist oft die größte Sicherheitslücke für Schadsoftware und Hacker:innen. Im Google Safety Engineering Center (GSEC) in München arbeiten Hunderte Expert:innen an Produkten, Diensten und Open-Source-Software, die das Internet für Nutzerinnen und Nutzer noch sicherer machen

Sicher surfen mit dem Chrome-Browser

»Wir stellen sicher, dass Datenschutz und -sicherheit in Googles Browser Chrome verankert sind. In den Einstellungen bieten wir die Möglichkeit, aus Optionen zu wählen, die den persönlichen Privatsphäre-Bedürfnissen entsprechen. Dort finden Nutzer:innen einen Leitfaden, in dem Einstellungen zu Cookies, Verlauf-Synchronisierung oder Safe Browsing erläutert werden. Die Safe-Browsing-Funktion hilft, wenn jemand im Begriff ist, gefährliche Webseiten zu besuchen oder potenziell Schadsoftware enthaltende Dateien herunterzuladen. Dann werden Warnungen eingeblendet. Mit dem Chrome-Sicherheitscheck lassen sich wichtige Sicherheitseinstellungen einfach prüfen: Sind kompromittierte Passwörter bekannt oder gibt es Browser-Erweiterungen, die potenziell Schadsoftware enthalten? Man findet den Sicherheitscheck in den Datenschutz- und Sicherheitseinstellungen des Chrome-Browsers.«

Sabine Borsay, Lead Produktmanagerin für Google Chrome ⟶ ***safety.google/chrome***

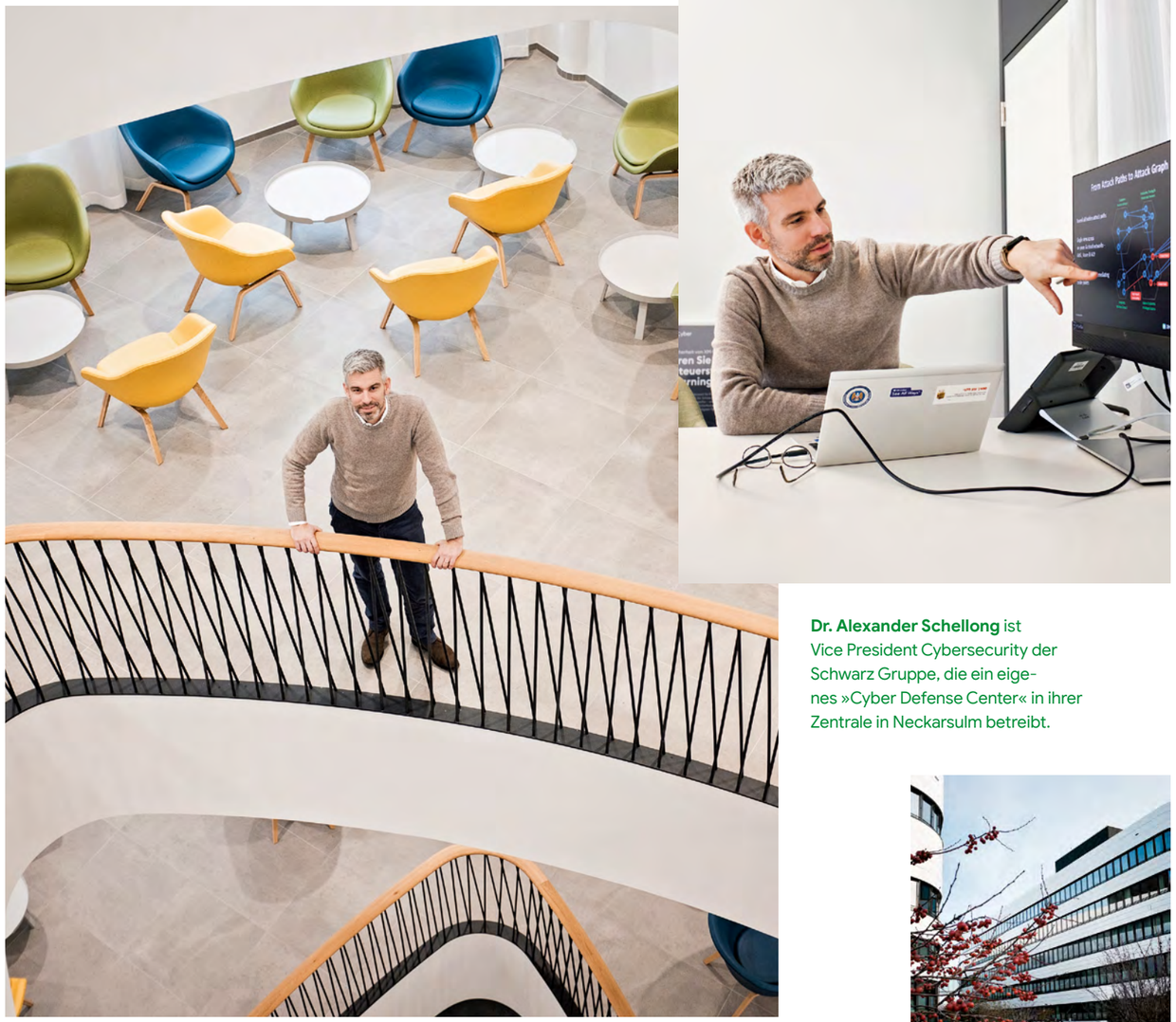
Schnellen Zugriff auf Daten ermöglichen

»Durch Befragungen und Studien haben wir herausgefunden, was Nutzerinnen und Nutzer von ihrem Google-Konto erwarten: Sie wollen zum Beispiel einen schnellen Zugriff auf Passwort, Profilbild oder andere persönliche Daten. Außerdem möchten sie sehen, falls irgendetwas mit ihrem Account nicht stimmt. Das Schöne ist, dass wir diese Nutzerbedürfnisse bereits erfüllen: Aus fast jedem Google-Produkt heraus kann man durch einen Klick aufs Profilbild oben rechts auf das Google-Konto zugreifen. Stellen wir fest, dass im Konto gespeicherte Passwörter kompromittiert und im Internet veröffentlicht sind, warnen wir Nutzerinnen und Nutzer – und stellen konkrete Abhilfe vor. Wir arbeiten stetig daran zu verstehen, ob neue Konzepte so funktionieren, wie wir uns das vorstellen. Wenn wir frühzeitig Probleme bei der Nutzung erkennen, können wir zusammen mit Nutzerinnen und Nutzern bessere Lösungen entwickeln – oder eine ganz andere Richtung einschlagen.«

Tobi Seitz, UX Researcher für das Google-Konto ⟶ ***goo.gle/googlekonto***

Fotos **MARIA HAEFNER, FLORIAN GENEROTZKY (3)**

Mehrere Tausend Angriffe pro Tag



Dr. Alexander Schellong ist Vice President Cybersecurity der Schwarz Gruppe, die ein eigenes »Cyber Defense Center« in ihrer Zentrale in Neckarsulm betreibt.

Der deutsche Einzelhandel ist immer häufiger von Cyberattacken betroffen und muss sich dagegen wappnen. Die Schwarz Gruppe, zu der unter anderem Lidl und Kaufland gehören, übernahm aus diesem Grund das israelische Unternehmen XM Cyber. Die neuen Geschäftsaktivitäten innerhalb der Unternehmensgruppe verantwortet Alexander Schellong

→ »Unsere Netzwerke werden mehrere Tausend Mal von Hacker:innen angegriffen – an jedem einzelnen Tag! Nach unserer Babynahrungsspende an die Ukraine erreichte die Zahl sogar kurzzeitig einen sechsstelligen Bereich. Das Spektrum ist breit, und wir stoßen immer wieder – sofern wir die Angriffe verfolgen können – auf Aktivitäten aus Russland, Belarus, China, Iran sowie Nordkorea. Manchmal versuchen Angreifer:innen, unsere Websites und Systeme durch eine große Anzahl an Anfragen in die Knie zu zwingen. Natürlich gibt es auch komplexe Angriffsversuche, die verschiedene Techniken und Schwachstellen kombinieren, um in unsere Systeme einzudringen. Wir nutzen verschiedene IT-Sicherheitslösungen, um die Angriffe abzuwehren. Zum Glück ist es bislang nicht gelungen, unsere Schutzmauern zu überwinden.

Ein vernetzter 24-Stunden-Betrieb

Cybersicherheit ist für unsere Unternehmensgruppe eine Herausforderung. Wir arbeiten vernetzt, was die Angriffsfläche erhöht. Zudem sind wir in 32 Ländern aktiv. Allein die 13 500 Lidl- und Kaufland-Filialen, der Lidl-Onlineshop und der Kaufland-Marktplatz vereinen Tausende Zulieferer und Partner. Durch automatisierte Systeme und die Cloud sind sie in Kontakt. Wenn unsere Filialen schließen, arbeiten die Warenlager weiter. Wir betreiben einen vernetzten 24-Stunden-Betrieb und versorgen ganz Europa und die USA.

Und dann sind da noch unsere 550 000 Mitarbeiterinnen und Mitarbeiter: Trotz der Spam-Filter, Fortbildungen und Hinweise, keine unbekannten Links zu öffnen, kann es vorkommen, dass jemand einen Anhang in einer der mehr als eine Million Phishing-Mails öffnet, die wir täglich erhalten.

Im ›Cyber Defense Center‹ in unserer Zentrale in Neckarsulm arbeitet ein großes Team von Kolleginnen und Kollegen rund um die Uhr. Es spielt eine zentrale Rolle für unsere IT-Sicherheit und ist Teil unseres globalen IT-Teams mit rund 4000 Mitarbeiterinnen und Mitarbeitern. In Neckarsulm haben wir auch ein eigenes Forensik-Labor, in dem wir zum Beispiel verdächtige IT-Komponenten genau untersuchen können. Dabei geht es nicht nur darum, akute Gefahren zu bannen, sondern auch zu lernen, wie wir in Zukunft unseren Schutz verbessern können.

Neben der Technologie ist für uns der Austausch mit anderen Unternehmen und mit Sicherheitsbehörden über die aktuelle Bedrohungslage sehr wichtig. Deswegen beraten wir uns mit Handelsunternehmen und Zulieferern weltweit.

Um IT-Security-Einsteiger zu fördern, bemühen wir uns am Bildungscampus Heilbronn schon heute um neue Ansätze. Der fehlende Nachwuchs ist für Behörden und Unternehmen eine große Herausforderung.

Trotz aller Anstrengungen wissen wir, dass Hacker:innen immer einen Schritt voraus sein werden. Deshalb ist es entscheidend, dass sie kein leichtes Spiel haben, falls sie wirklich einmal in unsere Infrastruktur eindringen. Um uns hier besser aufzustellen, haben wir Ende 2021 das israelische Unternehmen XM Cyber übernommen, das eine neue Perspektive in unser Sicherheitsdenken bringt, wie etwa diese Erkenntnis: Man kann Mauern so hoch bauen, wie man will, man muss davon ausgehen, dass Hacker:innen sie längst durchbrochen haben. XM Cyber hat eine weltweit anerkannte Expertise und simuliert kontinuierlich und ganzheitlich Hackerangriffe. Sie stellen dar, was Cyberkriminelle unternehmen könnten, um an die ›Kronjuwelen‹ zu kommen, ohne dabei unsere hoch kritischen IT-Systeme in Gefahr zu bringen.

Unternehmen sind unterschiedlich gut geschützt

Als Kronjuwelen werden sensible Daten oder Systeme bezeichnet, die keinesfalls in die Hände anderer fallen dürfen. Unsere Kundendaten gehören dazu, aber auch unsere Logistik darf nicht lahmgelegt werden: Denn fast alle Lkw und Waren sind miteinander vernetzt. Die Erkenntnisse von XM Cyber helfen uns, unsere Systeme so resilient zu machen, dass die sensibelsten Daten verschlossen bleiben. Bei über 2 Millionen Systemen, die XM Cyber bei Kunden analysierte, war dies in weniger als vier Schritten möglich.

So konnten wir bislang verhindern, dass Daten gestohlen oder unsere Systeme in Geiselhaft genommen wurden. Deutsche Unternehmen sind meinem Eindruck nach unterschiedlich gut geschützt. Viele sind schwach aufgestellt und Gefahren wie Ransomware-Angriffen ausgesetzt. Das kann das Geschäft für Wochen lahmlegen. Ich rate jedem, sich schnell mit IT-Sicherheit zu befassen. Viele Vorfälle können durch aufmerksames Handeln verhindert werden.«

46

Prozent der deutschen Unternehmen sind laut der Initiative »Deutschland sicher im Netz« 2021 mindestens einmal Opfer einer Cyberattacke geworden. Darunter versteht man den gezielten Angriff auf IT-Systeme oder -Infrastruktur, um diese lahmzulegen.

Fotos **EMANUEL HERM**

»Ich will etwas verändern«

Ornella Al-Lami arbeitet als Cybersecurity-Expertin in einem großen Unternehmen und kümmert sich dort um die Abwehr von Hackerangriffen. In ihrer Freizeit kämpft sie als »Hacktivistin« N3LL4 gegen digitale Gewalt, Mobbing und Schlimmeres und will vor allem denjenigen helfen, die sich selbst nicht wehren können

Dies könnte eine reichlich normale Geschichte sein. Der Artikel würde nun von einem jungen Mädchen handeln, das schon früh das Programmieren für sich entdeckt und in der sechsten Klasse das erste Praktikum in der IT-Branche macht.

Er würde über eine junge Programmiererin berichten, die zwar schon mit 13 Jahren als Entwicklerin jobbt, aber trotzdem eine Ausbildung zur Fachinformatikerin für Anwendungsentwicklung macht, weil ein offizieller Abschluss eben wichtig ist. Über eine Cybersecurity-Expertin, die im Schwachstellen-Management eines großen Unternehmens mit über 15 000 Mitarbeitenden beschäftigt ist. Zusammen mit ihren Kolleginnen und Kollegen schützt sie die IT-Infrastruktur vor unbefugtem Zugriff von außen. Dieser Text würde von unangekündigten Penetrationstests erzählen und von echten Hackerangriffen. Ein Brückenschlag zu jungen Frauen in der IT-Branche und Zahlen zum Fachkräftemangel wären sicher auch dabei.

Doch Ornella Al-Lami hat noch sehr viel mehr zu erzählen – einen kleinen Vorgeschmack darauf bekommt man auf ihrem Twitter-Profil. Unter dem Nickname N3LL4 lässt sie die über 70 000 Follower:innen an ihrem zweiten Leben, dem Engagement als Hacktivistin, teilhaben. Wer im Netz Opfer von Hatespeech, Cybermobbing oder Schlimmerem wird, kann sich an sie wenden. In den Untiefen des Webs sammelt sie für die Betroffenen Beweise und macht Täter:innen ausfindig, so lange, bis das Material für eine Anzeige ausreicht. Die Fälle, über die sie in 280 Zeichen berichtet, machen betroffen, wütend und sprachlos. Es sind die tiefsten Abgründe der digitalen Gesellschaft, aber alles andere als eine Seltenheit. Laut Angaben der Opferorganisation Weißer Ring ist bereits die Hälfte der Internet-User:innen Opfer von Cyberkriminalität geworden – neben Betrug sind sexuelle Belästigung und Cybermobbing besonders häufig.

Vom Computer in ihrer Wohnung jagt **Ornella Al-Lami** im Internet Verbrecher weltweit.

»Ich habe keine Angst, mir fehlt einfach der Selbstschutz«

Etwa 25 Stunden pro Woche kümmert sich Al-Lami um die Fälle – neben der Familie und dem Vollzeitjob im Schwachstellen-Management. Ihr Arbeitgeber kennt und befürwortet ihr Engagement. Geld nimmt sie für ihre Dienste nicht – im Gegenteil. Die Spenden, die sie manchmal für ihr Engagement bekommt, reichen kaum aus, um die Kosten für Technik und Co. zu decken. Die Differenz wird oft aus eigener Tasche beglichen. Bei der Frage nach dem Warum braucht Al-Lami trotzdem nicht lange zu überlegen. »Als mein Sohn geboren wurde, wuchs mein Bedürfnis, etwas zu verändern. Menschen zu helfen, mich gegen Cybergrooming, also sexuelle Belästigung, und Gewalt im Netz zu engagieren, mein eigenes Kind schon früh vor solchen Gefahren zu bewahren. Dagegen wird einfach zu wenig getan«, sagt die 24-Jährige. Unterstützung bekommt sie von einer Handvoll Helfer:innen, sie übernehmen die Kommunikation, sichten die 20 bis 30 Anfragen, die täglich über die Website reinkommen. Um die Open-Source-Recherche in sozialen Netzwerken oder dem Darknet, das Stöbern in den Quellcodes von Webseiten und andere Maßnahmen, die nötig sind, um Täter:innen aufzuspüren und aufzuhalten, kümmert sich die Hacktivistin allein.

So spürt sie einen jungen Mann auf, der vor laufender Kamera seine Mutter schlägt und Tiere quält – angefeuert von der eigenen Streaming-Community. Sie sammelt genug Material für eine Hausdurchsuchung bei einem Journalisten, der kinderpornografische Inhalte im Internet verbreitet. Sie findet die Betreiber eines rechten Webshops mit abstoßenden wie verfassungsfeindlichen Produkten.

Eigentlich wären Strafverfolgung und Ermittlungen auch im digitalen Raum Aufgabe des Staates. Doch wenn Polizei und Staatsanwaltschaft an ihre Grenzen stoßen, keine Ressourcen haben oder lange auf Genehmigungen warten müssten, braucht es eben Menschen, die selbst aktiv werden – sagt jedenfalls Al-Lami. Auch beim LKA und BKA scheint man, zumindest teilweise, dieser Meinung zu sein und arbeitet oft mit der Hackerin zusammen. Das Interesse ist schließlich das gleiche, Täter:innen aufzuhalten, aufzuspüren und schlimme Verbrechen im Netz zu verfolgen. Ungefährlich ist ihr Engagement nicht: Längst ist sie zur Zielscheibe von teils gefährlichen Kreisen geworden. »Ich habe keine Angst«, sagt die 24-Jährige. Als Mut will sie diese Eigenschaft aber nicht verstanden wissen. Es sei eher der fehlende Selbstschutz und alles andere als ein positiver Charakterzug. Sie kann nicht anders, nicht einfach wegsehen, Opfer vergessen, Täter:innen gewähren lassen. Und das liegt an ihrer eigenen Geschichte.

»Wie bekam er Zugriff auf meine Webcam?«

Als junges Mädchen wird Al-Lami von einem Stalker belästigt, einem älteren Mann, der sie immer wieder anspricht, ihr anzügliche Nachrichten schreibt. Lange unternimmt niemand etwas. Zum ersten Mal fühlt sie sich schutzlos ausgeliefert. Die Geschichte wiederholt sich, als Al-Lami das Internet für sich entdeckt. Ihre Webcam wird gehackt, ein älterer Mann will sie überreden, sich auszuziehen, wohlwissend, dass sie fast noch ein Kind ist. Dieses traumatische Erlebnis wird zu so etwas wie dem Ausgangspunkt ihres Hacktivismus. »Ich wollte verstehen, wie dieser Mann meine Webcam übernehmen konnte. Also habe ich mich eingelesen und viel selbst ausprobiert«, sagt Al-Lami. Anfangs nutzt sie ihr Wissen dazu, um den Mail-Account der Mutter zu knacken und sich in der Schule zu entschuldigen. Programmiersprachen wie Java, C, Python, HTML oder CSS bringt sie sich selbst bei, durch Ausprobieren und Austausch in Foren. Ihr Kampf gegen Pädokriminalität und Cybergrooming beginnt erst später, anfangs noch ganz ohne Hacking. Auf ihrem Instagram-Profil klärt sie über die Gefahren von unbedacht gepostete Kinderfotos auf – beim Baden im Pool, auf dem Wickeltisch, kurz vor dem Einschlafen. Schnell können solche Bilder auf Plattformen und Tauschbörsen für Pädophile landen, berichtet die 24-Jährige. Ihre Beiträge bekommen schnell viel Aufmerksamkeit. Zeitweise folgen über 100 000 Menschen ihrem Profil, es sind vor allem Eltern und Lehrkräfte. Gleichzeitig wird ihr Account mehrfach gesperrt. Ihre drastischen Inhalte und Warnungen passen schlecht in die heile Instagram-Welt. N3LL4 zieht zu Twitter um, die Arbeit verändert sich. Es gibt die ersten, verzweifelten Anfragen von Eltern, deren Kinder im Netz belästigt werden. Von Seiten der Behörden bekommen sie oft kaum Hilfe. Die Hackerin kann da schon mehr ausrichten.

»Ich habe schon oft ans Aufhören gedacht«

Oft reicht schon eine einfache Recherche in den sozialen Netzwerken, in Chats und Foren, im Code einzelner Webseiten. Viele Täter:innen sind arglos im Umgang mit ihren Daten. Die Beweise gehen direkt an die zuständigen Behörden, alles Weitere übernehmen im Optimalfall Staatsanwaltschaft und Polizei. Kommt es am Ende zu einer Verurteilung, sind Opfer nun besser geschützt, ist das der größte Lohn, ihre Motivation weiterzumachen, egal wie tief die Abgründe sind, in die sie blickt, egal wie viele Spuren die Fälle an der eigenen Seele auch hinterlassen. Und der Bedarf ist riesig. Die täglichen Anfragen nehmen immer mehr zu. Besonders Kinder und Jugendliche werden häufig Opfer im Netz. Bei einer Befragung aus Österreich gaben 27 Prozent der Minderjährigen an, im Internet schon einmal sexuell belästigt worden zu sein. Und laut einer Bitkom-Befragung wurden rund 15 Prozent der Jugendlichen in Deutschland Opfer von Cybermobbing – die Dunkelziffer dürfte deutlich höher sein, vermuten Fachleute. Für all diese Opfer könnte sich die Hacktivistin in Vollzeit engagieren oder direkt bei der Polizei anfangen. Beides kann sich Al-Lami kaum vorstellen. Dann hätte sie keinen Ausweg mehr, wenn ihr die Bilder, die Geschichten am Ende doch zu viel werden. »Ich will die Option haben, aufzuhören, von heute auf morgen, mich zurückzuziehen«, sagt sie. Im Moment sei das aber nicht möglich, sie werde zu sehr gebraucht.

Cyberkriminalität …

… eine weltweite Bedrohung.
Von fast jedem Ort auf der Welt können Kriminelle Systeme und digitale Geräte für ihre Machenschaften manipulieren. Das macht es schwer, ihre Spuren zu verfolgen.

15

Prozent der Jugendlichen in Deutschland wurden laut einer Bitkom-Umfrage Opfer von Cybermobbing – die Dunkelziffer dürfte deutlich höher sein, vermuten Fachleute.

Text **BIRK GRÜLING**

Illustration **JOE WALDRON** Foto **PRIVAT**

Safe and the City

Nicht nur Unternehmen sind ins Visier von Hackerangriffen geraten. Auch auf die kritische Infrastruktur des Landes haben es Cyberkriminelle immer häufiger abgesehen. Wir werfen einen Blick auf die aktuelle Lage und zeigen, wie gut Gemeinden und Kommunen darauf vorbereitet sind und wie sie gegen Angriffe kämpfen

⟶ Hochwasser, heftige Schneefälle, Waldbrände – das sind typische Ereignisse, bei denen Länder oder Gemeinden den Katastrophenfall ausrufen, weil »eine Beeinträchtigung bzw. eine unmittelbare Gefährdung für Leben oder Gesundheit einer Vielzahl von Menschen bzw. ein hoher Sachschaden« zu erwarten ist. So wie im Sommer 2021 im Landkreis Anhalt-Bitterfeld. Nur kam die Bedrohung dieses Mal aus dem Netz.

Es war das erste Mal in Deutschland, dass eine Kommune den Katastrophenfall aufgrund eines Cyberangriffs ausrief. Hacker:innen hatten sich Zugang zum IT-Netz der Kreisverwaltung verschafft und Schadsoftware eingeschleust, mit der sie Daten verschlüsselten – sogenannte Ransomware: Der Landkreis war wie gelähmt, konnte keine Sozialleistungen auszahlen, Autos anmelden oder Ausweise ausstellen. Das Ziel der Angreifer:innen: Geld zu erpressen, im Austausch gegen ein Programm, das die Daten wieder brauchbar macht.

Ransomware als größte Bedrohung

Aus Sicht des Bundesamts für Sicherheit in der Informationstechnik (BSI) gelten solche Ransomware-Angriffe aktuell als größte Bedrohung im Cyberbereich. Auch Angriffe auf Firewalls oder Router haben zugenommen – insbesondere seit dem Krieg in der Ukraine. Neben Unternehmen sind Städte und Kommunen ins Visier geraten.

»Auch auf uns gibt es immer wieder Angriffe«, sagt Laura Dornheim, IT-Referentin und Chief Digital Officer (CDO) der Stadt München. Sie ist sich der Risiken bewusst, sieht sich aber gut gewappnet: »Bisher hat unsere Verteidigung gehalten. Aber der Fall in Anhalt-Bitterfeld macht deutlich, dass diese Arbeit eben nicht nur eine theoretische Vorsorge ist.« Für Dornheim ist es ein Katz-und-Maus-Spiel: »Durch permanentes Monitoring müssen wir herausfinden, was gerade alles läuft, um schnell reagieren zu können.«

Haya Shulman ist Professorin für Informatik an der Goethe-Universität Frankfurt. Außerdem leitet sie eine

Text **KATHARINA FUHRIN**

Laura Dornheim ist IT-Referentin und Chief Digital Officer der Stadt München.

Abteilung am Fraunhofer-Institut für Sichere Informationstechnologie und koordiniert den Forschungsbereich »Analytics Based Cybersecurity« im Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE. Ihrer Erfahrung nach sind es vor allem drei Angriffsmuster, mit denen Kriminelle in Organisationen eindringen. Erstens: kompromittierte Passwörter. »Die Login-Daten sind der einfachste Weg, Organisationen zu infiltrieren. Fast alle Unternehmen sind früher oder später davon betroffen.« Zweitens: technische Schwachstellen in Systemen: »Angreifer:innen finden mit automatisierten Werkzeugen Lücken, durch die sie Organisationen infiltrieren können.« Drittens: »Malicious Insider«, also Mitarbeitende, die mit Kriminellen kooperieren. »Es gibt Gruppen, die solche Mitarbeiterinnen und Mitarbeiter mit viel Geld rekrutieren oder sogar gezielt über Bewerbungen einschleusen.«

Was passiert, wenn die Angreifer:innen erst mal im System sind, hängt von ihren Zielen ab. Vielen geht es um Erpressung wie in Anhalt-Bitterfeld, anderen um Cyberspionage oder um Sabotage. Corona hat es den Hacker:innen einfacher gemacht. Während der Lockdowns wurde auch in Behörden viel digitalisiert. Dadurch sind die Angriffsflächen größer geworden.

Das BSI unterstützt Kommunen

In München ist das IT-Referat für fast 50 000 Endgeräte verantwortlich. »Mit Beginn der Pandemie haben wir viele Mobilgeräte ausgegeben, um Homeoffice zu ermöglichen«, sagt Laura Dornheim. »Die Laptop-Quote liegt inzwischen bei über 90 Prozent. Das ist schon eine große Herausforderung, die alle auf dem aktuellen Stand zu halten.« Hinzu kommen viele Softwaresysteme, »da ist es normal, dass immer mal wieder Schwachstellen bekannt werden«. Manchmal stoßen Dornheim und ihr Team freitagabends darauf, arbeiten am Wochenende daran und sorgen montagmorgens dafür, dass alle 40 000 Angestellten der Stadt informiert sind und das Update aufgespielt wird.

Das IT-Referat in München ist mit mehr als 1400 Mitarbeitenden sehr groß und hat entsprechende Ressourcen. So betreibt die Stadt etwa zwei physisch getrennte Rechenzentren, die sich im Ernstfall gegenseitig ersetzen können. Andere Kommunen können sich diesen Aufwand nicht leisten.

Aber sie können sich Hilfe suchen. Das BSI unterstützt dabei, erprobte Maßnahmen umzusetzen, um so das Informationssicherheitsniveau zu steigern. Dafür empfiehlt das Amt kommunalen IT-Sicherheitsbeauftragten beispielsweise die Allianz für Cybersicherheit und das IT-SiBe-Forum zum Erfahrungsaustausch. Zudem gebe es bereits »IT-Grundschutzprofile«, bei denen konkrete Fälle und deren Lösung schablonenhaft abrufbar sind. Nach dem Angriff auf Anhalt-Bitterfeld startete das BSI Informationsveranstaltungen in verschiedenen Bundesländern, um unter anderem auf die Profile aufmerksam zu machen.

Für Haya Shulman klingt ein anderer Weg erfolgversprechender: konsequentes Outsourcing an Dienstleister. In einer Studie hat das Fraunhofer SIT 2020 die Sicherheit von Parteien in Deutschland und Israel verglichen. Israel schnitt deutlich besser ab. »Eine eigene Infrastruktur ist eine große Sicherheitslücke. In Israel ist es üblich, die IT-Sicherheit an externe Dienstleister zu geben. Das ist nicht nur effizient, sondern auch günstiger.« Sie empfiehlt Unternehmen und Behörden, periodische Scans auf schwache Passwörter und Schwachstellen zu machen, also selbst die Rolle von Hacker:innen einzunehmen. Auch dafür gibt es Dienstleister.

Triviale Passwörter, Rechner im tagelangen Standby-Betrieb, unachtsames Herausgeben von Zugangsdaten – meistens gelangen Hacker:innen durch Fehler von Mitarbeiterinnen und Mitarbeitern ans Ziel. Auch in Anhalt-Bitterfeld war es sehr wahrscheinlich eine Phishing-Mail, die das Tor ins System öffnete und zu einem fast sieben Monate dauernden Katastrophenfall führte, nachdem der Landrat sich gegen eine Lösegeldzahlung entschieden hatte.

In München setzt Laura Dornheim daher künftig noch mehr auf Schulungen der Mitarbeiterinnen und Mitarbeiter. »Der menschliche Faktor war lange nicht so im Fokus bei der IT-Sicherheit, weil man dachte, das kann man technisch abfangen. Aber genauso muss man die einzelnen Nutzerinnen und Nutzer abholen und ihnen klarmachen, dass alle gemeinsam eine Verantwortung mittragen, die Stadt sicher zu halten.«

Gleichzeitig geht die Entwicklung hin zu einer »Zero-Trust-Architektur«, bei der durch eine strengere Authentifizierung nicht das ganze Netz, sondern einzelne Server geschützt werden. In den USA müssen Bundesbehörden Zero-Trust bis 2024 umsetzen. Haya Shulman leitet ein Projekt mit dem Ziel, eine Referenzarchitektur zu entwickeln, die für deutsche Organisationen und Kommunen passt. Durch den Zero-Trust-Ansatz »vertraut« ein Rechner nicht mehr automatisch anderen Rechnern im selben Netz, sondern muss sich durch weitere Kontrollen authentifizieren: Wenn sich Angreifer:innen wie in Anhalt-Bitterfeld Zugang verschaffen, stehen sie vor der nächsten verschlossenen Tür.

Haya Shulman ist u. a. Professorin für Informatik an der Goethe-Universität Frankfurt.

207

Tage – so lange konnten nach dem **Ransomware-Angriff** in Anhalt-Bitterfeld keine bürgernahen Dienstleistungen erbracht werden.

Illustration **JOE WALDRON** Fotos **PR**

»Wir wollen hin zu einer Umgebung, die maximale Sicherheit bietet«

Mithilfe einer Multi-Cloud will Markus Richter, IT-Beauftragter der Bundesregierung, die Digitalisierung der Verwaltung beschleunigen. Eine Vielzahl von Anwendungen unterschiedlicher Anbieter soll künftig zentral verfügbar sein – und einen noch besseren Schutz der Bürgerdaten gewährleisten

Interview **CHRISTIAN BAULIG**

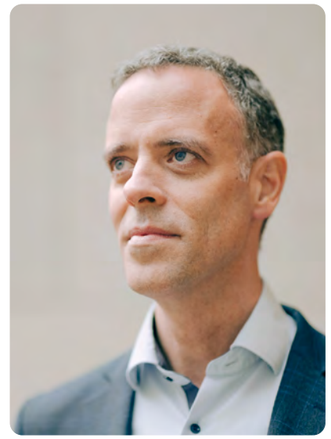
⟶ Herr Richter, die Bundesregierung möchte künftig mehr Daten der Verwaltung in der Cloud speichern und verarbeiten. Was planen Sie konkret?
Die von Bund und Ländern verabschiedete Strategie sieht vor, dass wir eine sogenannte Multi-Cloud implementieren, in der viele verschiedene Anwendungen unterschiedlicher Anbieter gebündelt sind. Im Herbst haben wir daher in einem Pilotprojekt eine Koordinierungsstelle eingerichtet und einzelne Dienste getestet.

Was versprechen Sie sich von einer solchen Multi-Cloud?
Wir schaffen Auswahlmöglichkeiten, wahren den Wettbewerb und profitieren von Innovationen. Da die Dienste auf verschiedenen Cloud-Plattformen laufen, können wir schnell und kostengünstig eine Vielzahl von Arbeitsplätzen ausstatten. Zugleich hilft uns die Multi-Cloud, von vielen kleinen Rechenzentren wegzukommen hin zu einer Umgebung, die maximale Skalierbarkeit und Sicherheit bietet.

Wie gewährleisten Sie diese Sicherheit?
Sämtliche Anwendungen müssen die Anforderungen des Bundesamts für Sicherheit in der Informationstechnik erfüllen. Natürlich ist dabei auch der europäische Rechtsrahmen einzuhalten. Zudem bietet die Multi-Cloud die Möglichkeit, Daten und Programme von einem Speicherplatz zu einem anderen zu verschieben, falls die Situation das einmal erfordern sollte.

Welche Aufgabe hat die von Ihnen erwähnte Koordinierungsstelle?
Sie ist die Spinne im Netz. Wenn eine Behörde in Deutschland einen Bedarf für einen IT-Service hat, wendet sie sich an die Koordinierungsstelle. Diese fragt zunächst im Verbund der öffentlichen Dienstleister, ob jemand diesen Bedarf decken kann. Ist das nicht der Fall, wird der Service ausgeschrieben. Derzeit werten wir die Ergebnisse des Pilotprojekts aus und gehen danach in die Umsetzung.

Bislang hinkt Deutschland, was die Digitalisierung der Verwaltung angeht, seinen Zielen hinterher: Von 600 Leistungen, die laut Onlinezugangsgesetz bis Ende 2022 komplett digitalisiert sein sollten, war zum Stichtag nicht einmal die Hälfte verfügbar.
Es ist richtig, dass wir das gesteckte Ziel nicht erreicht haben. Trotzdem muss man festhalten, dass wir gerade in den letzten Monaten deutliche Schritte nach vorne gegangen sind: Ummeldung, Bauantrag, BAföG – zahlreiche Leistungen, die viele Menschen betreffen,



sind mittlerweile online verfügbar. Wir stellen fest, dass es beim Ausrollen weniger um Technik geht als vielmehr um Change Management. Die Prozesse müssen angepasst werden, und das ist ein dickes Brett.

Wann wird denn die Multi-Cloud in Betrieb gehen?
Im Laufe dieses Jahres werden wir erste Ausschreibungen starten. Es gibt jedoch keine Stunde null, zu der alles gleichzeitig startet. Es wird vielmehr ein Prozess sein, dessen genauen Zeitplan wir noch erarbeiten müssen. Aktuell ist der Markt stark in Bewegung, und die großen Anbieter haben noch einige Hausaufgaben zu erledigen.

Sie spielen auf das Thema »Souveränität« an. Was verstehen Sie darunter und warum ist sie so wichtig?
Souveränität ist die Grundvoraussetzung. Ich bin froh, dass aktuell zwischen der EU-Kommission und den USA entsprechende Abstimmungen laufen. Die neue Presidential Order trägt den europäischen Anforderungen bereits Rechnung. Unternehmen wie Google, Microsoft oder Amazon empfehle ich, sich ebenfalls abzustimmen, was Schnittstellen beziehungsweise Standards anbelangt. Für uns ist aber wichtig, dass Open Source eine große Rolle spielen wird.

Was wird die Multi-Cloud die Bürgerinnen und Bürger kosten?
Das Modell sieht vor, dass die Anbieter den Aufbau selbst vornehmen und wir über Lizenzen Abrufe starten. Wir ziehen also kein Rechenzentrum hoch, in das wir die Cloud einbauen lassen. Die genauen Kosten hängen stark davon ab, wie groß der konkrete Bedarf an Services und Infrastruktur sein wird. Dafür werden wir noch Abfragen bei den Ländern und auch auf Bundesebene machen.

Fotos **LENA GIOVANAZZI**

Treibt die Digitalisierung der öffentlichen Verwaltung des Bundes voran: **Markus Richter.**

Zur Person

Dr. Markus Richter ist seit Mai 2020 Beauftragter der Bundesregierung für Informationstechnik im Rang eines Staatssekretärs im Bundesministerium des Innern und für Heimat.
Als »Bundes-CIO« ist Richter zentraler Ansprechpartner in übergreifenden IT-Fragen der öffentlichen Verwaltung des Bundes und verantwortet die Steuerung der Informationstechnik und Digitalisierung der Bundesverwaltung.
Zuvor war der 46-jährige Jurist fast 15 Jahre im Bundesamt für Migration und Flüchtlinge tätig, von 2018 bis 2020 als Vizepräsident.

»Sicherheit und Souveränität sind zwei Seiten einer Medaille«

Immer höhere Sicherheitsstandards – zu immer niedrigeren Kosten: Daran arbeiten Expert:innen bei Google.

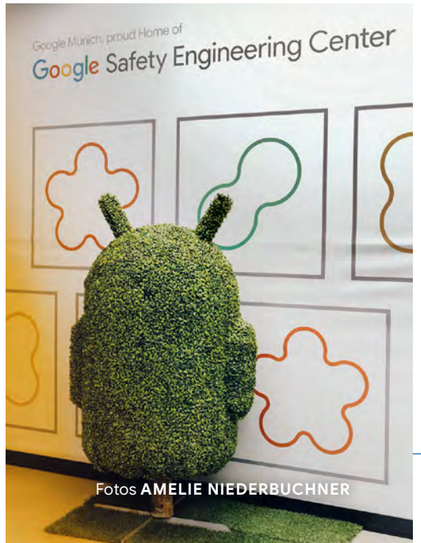
Die Cloud spielt eine entscheidende Rolle, wenn Unternehmen ihre Infrastruktur vor Cyberangriffen schützen wollen, sagt Wieland Holfelder, Vice President Engineering bei Google. Darüber hinaus bietet die Cloud die Möglichkeit, die Digitalisierung zu beschleunigen

⟶ »Unternehmen sind heutzutage vielfältigen Cyberbedrohungen ausgesetzt. Ihre Infrastruktur vor Angriffen oder gar Verlusten zu schützen ist essenziell, um ihre Existenz zu sichern. Insbesondere wenn IT-Sicherheit nicht zum Kerngeschäft einer Firma gehört, ist es sehr aufwendig, Technologien und Software stets auf dem aktuellsten Stand zu halten.

All diese Herausforderungen nimmt die Cloud Unternehmerinnen und Unternehmern ab. Hunderte Expertinnen und Experten erweitern die Cloud bei uns fortlaufend um neue Funktionen, die einen immer besseren Schutz bieten. Unsere Innovationsgeschwindigkeit ist dadurch sehr hoch. Jedes Sicherheitsupdate, das wir unseren Kunden zur Verfügung stellen, umfasst Wissen aus einer Bedrohung, einer Schwachstelle oder einer neuen Angriffstechnik. Dadurch besitzt die Cloud eine Art digitales Immunsystem.

Unsere Kunden profitieren auch von Skalierungseffekten: Die Kosten, die sie für die Sicherheit ihrer Infrastruktur und ihrer Daten investieren müssen, sinken. Gleichzeitig werden die Sicherheitsstandards, die sie hierfür erhalten, immer höher. Darüber hinaus haben sie auch die Möglichkeit, Kapazitäten jederzeit hochzufahren und beispielsweise mehr Speicherplatz oder schnellere Rechenleistungen in Anspruch zu nehmen. Ganz nach ihren individuellen Bedürfnissen.

Früher hatten Unternehmen häufig Bedenken, die Cloud zu nutzen – und manche haben diese Bedenken vielleicht bis heute: Sie haben Sorge, sich von einem bestimmten Anbieter abhängig zu machen, oder stehen der Frage skeptisch gegenüber, wer Zugriff auf ihre Daten hat, wo genau sie gespeichert sind und wie sie verschlüsselt werden. Manch einer fragt sich auch, was mit seinen Daten passiert, wenn die Google Cloud einmal ausfallen sollte.



Fotos **AMELIE NIEDERBUCHNER**

Wir nehmen diese Bedenken rund um das Thema ›Digitale Souveränität‹ sehr ernst und haben spezielle Produkte entwickelt, die diese Bedenken und das Sicherheitsbedürfnis unserer Kunden adressieren. Wir nennen das Sovereign Cloud. Das erste Sovereign-Cloud-Produkt, das wir 2022 auf den Markt gebracht haben, heißt Sovereign Controls und garantiert, dass Kundendaten in der deutschen Region von Google Cloud gespeichert und verschlüsselt werden und nicht in andere Länder verschoben werden können. Die Schlüssel werden dabei außerhalb der Google-Infrastruktur gespeichert und verwaltet. So gewährleisten wir, dass Unbefugte keinen Zugriff darauf bekommen. Da Google auf Open Cloud und Open Source setzt, gibt es auch Möglichkeiten, Workloads auf andere Plattformen zu migrieren, sollte dies gewünscht oder notwendig sein.

Die gesamte Lösung im Blick

Sicherheit und Souveränität gehören für uns zusammen. Ich sage gerne, dass es zwei Seiten einer Medaille sind. Wenn Sie zum Beispiel durch einen Hackerangriff Ihre Daten verlieren, ist auch Ihre Souveränität dahin. Und wenn Sie nicht souverän agieren können, ist es schwierig bis unmöglich, die eigene Sicherheit zu garantieren. Beide Themen gehören zum Kern unserer Strategie, und wir bieten Lösungen für die Cloud nach europäischen Datenschutzregeln.

Bislang haben Cloud-Anbieter nach dem Prinzip ›Geteilte Verantwortung‹ agiert, der Cloud-Anbieter war für die Sicherheit der Infrastruktur zuständig, der Kunde für die Sicherheit der Anwendungen, die darauf laufen. Mittlerweile arbeiten wir bei Google Cloud nach einem Modell, das wir ›Geteiltes Schicksal‹ nennen. Es geht also nicht mehr nur um geteilte Verantwortung, sondern wir übernehmen inzwischen auch Verantwortung und leisten Hilfestellung für die Gesamtlösung. Das geht so weit, dass es sogar günstigere Cybersecurity-Versicherungen gibt, wenn Kunden mit Google Cloud arbeiten.

Das zunehmende Vertrauen, das die Nutzerinnen und Nutzer Cloud-Lösungen entgegenbringen, treibt den Übergang in die Cloud voran. Das führt zu noch größerer Sicherheit für alle.

Ich bin davon überzeugt, dass wir die Digitalisierung und die Datensicherheit in den Unternehmen in Deutschland – von klein bis groß – nur mithilfe der Cloud weiter vorantreiben können: Denn nur die Cloud bietet Unternehmerinnen und Unternehmern die Möglichkeit, ihre Kapazitäten jederzeit flexibel an ihre individuellen Bedürfnisse anzupassen. Und das bei höchstmöglicher Sicherheit und Souveränität.«

Zur Person

Dr. Wieland Holfelder ist Vice President Engineering bei Google und leitet das Google Safety Engineering Center in München, wo auch an der Google Cloud gearbeitet wird.

Kann Technologie die Demokratie schützen?

Egal ob es um das private Onlinebanking, die Digitalisierung der Verwaltung oder die Vernetzung von Fabriken geht: In allen Bereichen lauern Cyberrisiken, die bei vielen Menschen zu Verunsicherung führen. Privatpersonen, Unternehmen und Organisationen müssen sich zunehmend vor diesen Risiken schützen: Hacker:innen geht es längst nicht mehr nur darum, Daten zu klauen. Immer häufiger wollen sie auch demokratische Strukturen angreifen

⟶ Der russische Angriffskrieg auf die Ukraine hat in den vergangenen Monaten gezeigt, wie gewaltig die Konflikte sind, die im Cyberspace ausgetragen werden. Längst werden Kriege nicht mehr nur in den Städten und Dörfern geführt, sondern mittels Cyberattacken auch im Netz.

Laut einem Bericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) hat das vergangene Jahr gezeigt, »dass unvorhergesehene Ereignisse die Bedrohungslage auf ein neues Level heben können und Kollateralschäden durch Cyberangriffe in Nachbarländern auch unmittelbare Auswirkungen auf Deutschland haben können«. Im digitalen Raum seien die Bedrohungen derzeit so groß wie nie, schreibt das BSI.

Darüber hinaus stellen Cyberangriffe auf Unternehmen in Deutschland eine Gefahr für unsere Gesellschaft dar. Der Schaden beläuft sich für das Jahr 2022 geschätzt auf mehr als 200 Milliarden Euro. Zu den meistgenutzten gehören Ransomware-Attacken, bei denen Daten verschlüsselt und erst gegen Zahlung eines Lösegeldes wieder freigegeben werden. Und DDoS-Attacken, bei denen ein Server mit Anfragen überhäuft wird, bis er zusammenbricht.

Neben wirtschaftlichen Schäden mit hohen Kosten ist auch die kritische Infrastruktur in Gefahr. Dies kann im schlimmsten Fall den gesellschaftlichen Frieden bedrohen. Auch Webseiten deutscher Behörden wurden bereits attackiert, darunter die der Bundespolizei, mehrerer Landespolizeibehörden und des deutschen Bundestags. So wird deutlich, in welchem Ausmaß Software heutzutage als Waffe genutzt werden kann: gegen Privatpersonen, Unternehmen, Medien oder Regierungen.

In der Vergangenheit haben viele versucht, sich alleine gegen Cyberattacken abzuschotten. Doch geschlossene Systeme machen es für den Einzelnen immer schwieriger, sich alleine gegen wachsende Gefahren zu schützen. Größere Sicherheit verschaffen Cyberlösungen, die auf offenen, hochsicheren Standards beruhen und eine enge und transparente Zusammenarbeit zwischen den Akteuren in der Sicherheitsindustrie fördern. Kurzum: das Prinzip der Open Security – ein Konzept, auf das auch Google setzt.

Was steckt hinter Open Security?

Ein solch offener Ansatz mag zunächst paradox klingen, doch in unserer heutigen mobilen, hybriden Umgebung ist Cybersecurity ein Teamsport, und gemeinsam kann man höhere Standards für die Sicherheit setzen, von denen alle profitieren. Ein wichtiges Prinzip der Open Security besteht im sogenannten Zero-Trust-Modell: eine Vorgehensweise, bei der alle Nutzer:innen, alle Geräte und Anwendungen kontinuierlich auf Sicherheitsrisiken überprüft werden.

So wird die Gemeinschaft geschützt – und damit auch jedes einzelne Mitglied. Ihr gemeinsames Ziel besteht darin, Hacker:innen keine Chance zu geben – und damit demokratische Strukturen zu stärken.

Doch Cybersecurity ist kein Thema, das irgendwann erledigt ist. Dauerhafter Schutz erfordert kontinuierliche Weiterentwicklung. Aus diesem Grund investiert Google in europäische Standorte mit dem Ziel, Europa zur Heimat seiner weltweiten Bemühungen im Bereich Cybersecurity zu machen.

Inwiefern fördert Google den Ausbau der Cybersecurity in Europa?

Sicherheit war schon immer der zentrale Aspekt der Google-Produkt-Strategie. Das Unternehmen arbeitet kontinuierlich daran, weltweit führende Sicherheitslösungen für alle anzubieten: Privatpersonen, Unternehmen, Politik und Verwaltung ⟶

Distributed Denial of Service

Ein Distributed Denial of Service, kurz DDoS-Angriff, ist ein bösartiger Versuch, den Server einer Person oder einer Organisation mit Angriffs-Traffic zu überfluten. So wird verhindert, dass legitimer Traffic einen Dienst erreicht. Hierfür infizieren Hacker:innen mehrere zusammengeschaltete Geräte mit Schadsoftware. Je mehr Rechner zusammengeschaltet werden, desto schlagkräftiger ist der Angriff.

Text **CHRISTIANE MANOW-LE RUYET** Illustration **JOE WALDRON**

Threat Intelligence

Threat Intelligence beschreibt den gesamten Prozess, um Cyberbedrohungen zu identifizieren und zu untersuchen. Dabei werden Daten analysiert, um Probleme, Angriffsmethoden und Angreifer:innen aufzudecken, um damit spezifische Lösungen entwickeln zu können, die Systeme in Zukunft sicherer machen.

sollen sich im Internet stets in einem geschützten Umfeld bewegen. Um dies noch weiter auszubauen, entwickeln Hunderte Expert:innen in den Google Safety Engineering Centern technische Lösungen und Produkte, teilen Wissen über IT-Sicherheit und tauschen sich mit anderen Unternehmen und Organisationen aus. Am Standort München kümmern sich Expert:innen um die Themen Datenschutz und Sicherheit. Am Standort Dublin geht es in erster Linie darum, Strategien für den verantwortungsvollen Umgang mit Inhalten zu entwickeln. Im spanischen Málaga eröffnet demnächst ein weiterer Standort. Das Ziel: Nutzer:innen, Expert:innen, Unternehmer:innen und Politiker:innen zusammenbringen, um die digitale Sicherheit Europas gegen wachsende Bedrohungen zu stärken und so die Demokratie durch enge Zusammenarbeit zu schützen. Dazu gehört auch, dass Menschen Informationen aus einer Vielzahl an glaubwürdigen Quellen finden.

Mit welchen Maßnahmen stellt Google den Zugang zu verlässlichen Informationen sicher?

Die Kontrolle von Medien und Journalist:innen war und ist ein entscheidendes Werkzeug für autokratische Systeme und Diktatoren, um Menschen davon abzuhalten, sich ihre eigene Meinung zu bilden.

Das zeigte etwa der Angriff auf die unabhängige russische Zeitung *Novaya Gazeta* im Herbst 2021: 1,2 Millionen Server-Zugriffe pro Sekunde legten damals die Server der Zeitung, und damit ihren Online-Auftritt, lahm. Ein sogenannter DDoS-Angriff – ausgerechnet an einem der letzten Tage der russischen Parlamentswahlen.

Ein Projekt, das Websites vor derartigen DDoS-Angriffen schützt, ist »Project Shield«. Es wurde 2013 von Jigsaw entwickelt – einer Tochter von Google, die sich insbesondere mit der Bekämpfung von Extremismus, Onlinezensur und Cyberattacken beschäftigt.

Project Shield wird derzeit in über 100 Ländern eingesetzt und schützt Tausende von Webseiten, beispielsweise in der Ukraine. Dazu wird der Traffic, der auf einer Website landen sollte, vorübergehend auf das deutlich resilientere Google-Netzwerk umgeleitet. Potenziell schadhafte Anfragen, etwa solche von DDoS-Attacken, werden herausgefiltert und nur vertrauenswürdige Anfragen an die eigentliche Website weitergeleitet. Google stellt sich also wie ein Schutzschild vor die betreffende Website. Dadurch wird eine Überlastung der Server verhindert, und Nutzer:innen können weiterhin auf vertrauenswürdige Informationen zugreifen.

Natürlich gibt es für undemokratische Akteure andere Wege, die Verlässlichkeit von Informationen zu bedrohen. Beispielsweise indem sie gezielt Fehlinformationen verbreiten. Auch dies ist eine Methode, die immer stärker zunimmt.

Wie können Menschen sich vor Fehlinformationen schützen?

Das sogenannte Pre-Bunking ist eine Kommunikationstechnik, die entwickelt wurde, um Menschen dabei zu unterstützen, ein »mentales Immunsystem« aufzubauen, das ihnen dabei hilft, solche Fehlinformationen besser zu erkennen und damit Resilienz gegen Manipulationstechniken und Fehlinformations-Narrative aufzubauen.

Beim Pre-Bunking werden Menschen Videos gezeigt, in denen sie erfahren, woran sich irreführende Argumente und bewusst gestreute Fehlinformationen erkennen lassen.

Jigsaw startete hierzu 2022 eine Kampagne in mehreren zentral- und osteuropäischen Ländern. Sie zielte darauf ab, der Verbreitung von Fehlinformationen entgegenzuwirken, die beispielsweise über geflüchtete Menschen aus der Ukraine im Umlauf waren.

Und das Konzept funktioniert: Tests belegen, dass Menschen, die solche Pre-Bunking-Videos gesehen haben, richtige Informationen von falschen besser unterscheiden können. Pre-Bunking kann damit zu einem wichtigen Bestandteil werden, um demokratische Werte zu sichern.

Trotz aller Anstrengung im Kampf gegen Hackerangriffe, die Verbreitung von Fehlinformationen und den Angriff auf demokratische Strukturen ist aus Sicht von Royal Hansen, Vice President of Engineering for Privacy, Safety and Security und Leiter des globalen Entwicklungsteams für Datenschutz und -sicherheit bei Google, vorerst keine Entspannung in Sicht: »Es reicht nicht aus, der Bedrohung nur ein paar Schritte voraus zu sein«, fasst er die Situation zusammen. »Wir müssen alle zusammenarbeiten, um die Zukunft eines offen zugänglichen, freien, globalen, interoperablen, verlässlichen und sicheren Internets zu schützen. Sei es durch die Bekämpfung von Cyberbedrohungen, durch die Entwicklung sicherer Technologien, die das volle Potenzial der Gesellschaft freisetzen, oder durch die Entwicklung verantwortungsvoller Technologie-Richtlinien.«

Quantenoptik, KI-Software & Co.

Die Bekämpfung von Cyberkriminalität spielt weltweit eine große Rolle – auch in Deutschland. Zahlreiche Start-ups arbeiten hierzulande an Lösungen, um die Sicherheit für alle im Netz zu erhöhen. Wir stellen drei von ihnen vor

1. PASSWÖRTER WERDEN ÜBERFLÜSSIG

Wer? Jannis Froese und Nils Vossebein haben mit DeepSign eine schnellere, sichere Alternative zur Zwei-Faktor-Authentifizierung für Website- und App-Log-ins entwickelt.

Was? DeepSign macht auf dem Handy abzulesende Passwörter und Codes überflüssig. Stattdessen erkennt die Software PC-Nutzer:innen an ihren individuellen Maus- und Tastaturbewegungen, etwa der Tipp- oder Reaktionsgeschwindigkeit oder dem Scroll-Verhalten. Dieses Verhalten ist so einzigartig wie ein Fingerabdruck.

Wozu? DeepSign beschleunigt den Authentifizierungsprozess und ermöglicht eine lückenlose Verifizierung befugter Nutzer:innen. Die Technologie ist privat wie in Unternehmen einsetzbar, aber auch in Produktion und Forschung.

Mehr Infos: ***deepsign.de***

2. VERSCHLÜSSELUNG MIT QUANTENOPTIK

Wer? Aus dem Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF heraus haben Dr. Oliver de Vries und Dr. Kevin Füchsel das Quantentechnologie-Start-up Quantum Optics Jena (QOJ) gegründet, um Kommunikationssysteme sicherer zu machen.

Was? Die besondere mathematische Leistungsfähigkeit von Quantencomputern, die Expert:innen in Zukunft entwickeln werden, wird die Leistung konventioneller Computer um ein Vielfaches übersteigen. Sie sind daher eine potenzielle Bedrohung für die heute verwendeten Verschlüsselungsverfahren bei der Datenübertragung. QOJ nutzt eine neue Verschlüsselungsmethode, bei der nur Sender:in und Empfänger:in und niemand Externes die Daten auslesen können. So soll die Datenübertragung auch in Zukunft sicher bleiben.

Wozu? QOJ wird in der Forschung genutzt und bald Regierungen und Energieversorgern oder Finanz- und Gesundheitseinrichtungen dabei helfen, Cyberattacken abzuwehren.

Mehr Infos: ***qo-jena.com***

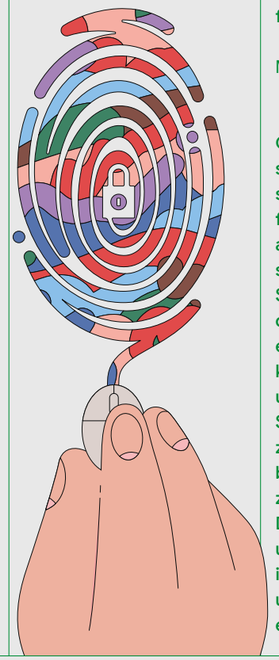
3. MALWARE AUFSPÜREN

Wer? Julian Ziegler und Christian Boll haben mit Inlyse eine KI-Software entwickelt, die Malware und Cyberangriffe in Sekundenschnelle identifiziert.

Was? Inlyse nutzt neuronale Netze, um Malware aufzuspüren. Dazu verwandelt die Technologie Daten in Bilder, die dann von den neuronalen Netzen interpretiert werden. Sie erkennen kleinste Hinweise auf Computerviren und auch unbekannte Bedrohungen sofort.

Wozu? Inlyse soll künftig Privatpersonen und Unternehmen zuverlässigen, aber erschwinglichen Schutz vor Cyberbedrohungen ermöglichen. Inlyse ist im Browser, für E-Mails sowie für Programme nutzbar.

Mehr Infos: ***inlyse.com***



Google engagiert sich nicht nur selbst im Bereich Cybersecurity, sondern fördert in der **Google for Start-Ups Growth Academy** auch junge Gründer und vernetzt sie mit der globalen Google Start-Ups Community. In einem dreimonatigen Programm erhalten sie notwendige Fähigkeiten, die sie brauchen, um ihr Geschäft auszubauen. Sie arbeiten mit Mentoren zusammen. GSEC-Expert:innen bieten regelmäßig Schulungen zur Datenanonymisierung, Datenschutz im Produktdesign und beraten Gründer:innen in Fragen zu Datenschutz und Privatsphäre in der Produktentwicklung.

Illustration **CAMILO HUINCA**

Der erste Internetwurm der Geschichte
Angeblich aus Versehen führte der US-Amerikaner Robert Tappan Morris einen Zusammenbruch des Internets herbei.

Massachusetts Institute of Technology
2.11.1988

Robert Tappan Morris

⟶ Am 2.11.1988 hielten Experten das Internet für zerstört. Grund dafür war ein Programm, das der Informatik-Student Robert Tappan Morris entwickelt hatte, um zu ermitteln, wie viele Rechner an das Internet angeschlossen sind: Es sollte durch eine Sicherheitslücke in die Rechner eindringen, einen Zählwert versenden und sich dann auf weitere Rechner kopieren. Doch das ging schief: Das Programm drang gleich mehrfach in jeden Rechner ein und führte zu einer besonders hohen Auslastung des gesamten Netzwerks, bis es schließlich zusammenbrach. Der erste Internet-Wurm war geboren. Morris beteuerte, dass dies keine Absicht gewesen sei. Trotzdem war er der erste Mensch, der wegen Computermissbrauchs verurteilt wurde: Er erhielt eine dreijährige Bewährungsstrafe, musste 400 Sozialstunden leisten und eine Geldstrafe von 10 050 US-Dollar zahlen. Ein Gutachter schätzte damals, dass etwa 10 Prozent des Internets durch den Wurm ausgefallen waren. Seit 1999 lehrt Robert Tappan Morris als Professor am Massachusetts Institute of Technology (MIT). Dort, wo er den Wurm entwickelt hatte.

Foto **PICTURE ALLIANCE / ASSOCIATED PRESS | MICHAEL J. OKONIEWSKI**

IMPRESSUM
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland | Tel.: +353 1 543 1000 | Fax: +353 1 686 5660 | E-Mail: support-deutschland@google.com | Geschäftsführung: Elizabeth M. Cunningham, David M. Sneddon | Google Ireland Limited ist eine nach irischem Recht gegründete und registrierte Gesellschaft | Registernummer: 368047 | Umsatzsteuer-ID.-Nr.: IE6388047V

Dies ist eine Anzeigensonderveröffentlichung von Google. Hergestellt in Deutschland. Papier: LEIPA MAG PLUS gloss; Druck: Evers-Druck GmbH - ein Unternehmen der Eversfrank Gruppe. Danke an das Team von SZ Scala GmbH.

BLAUER ENGEL DAS UMWELTZEICHEN GU9
www.blauer-engel.de/uz195
- ressourcenschonend und umweltfreundlich hergestellt
- emissionsarm gedruckt
- überwiegend aus Altpapier

Dieses Druckerzeugnis ist mit dem Blauen Engel ausgezeichnet.


target....)
assign
null
Google