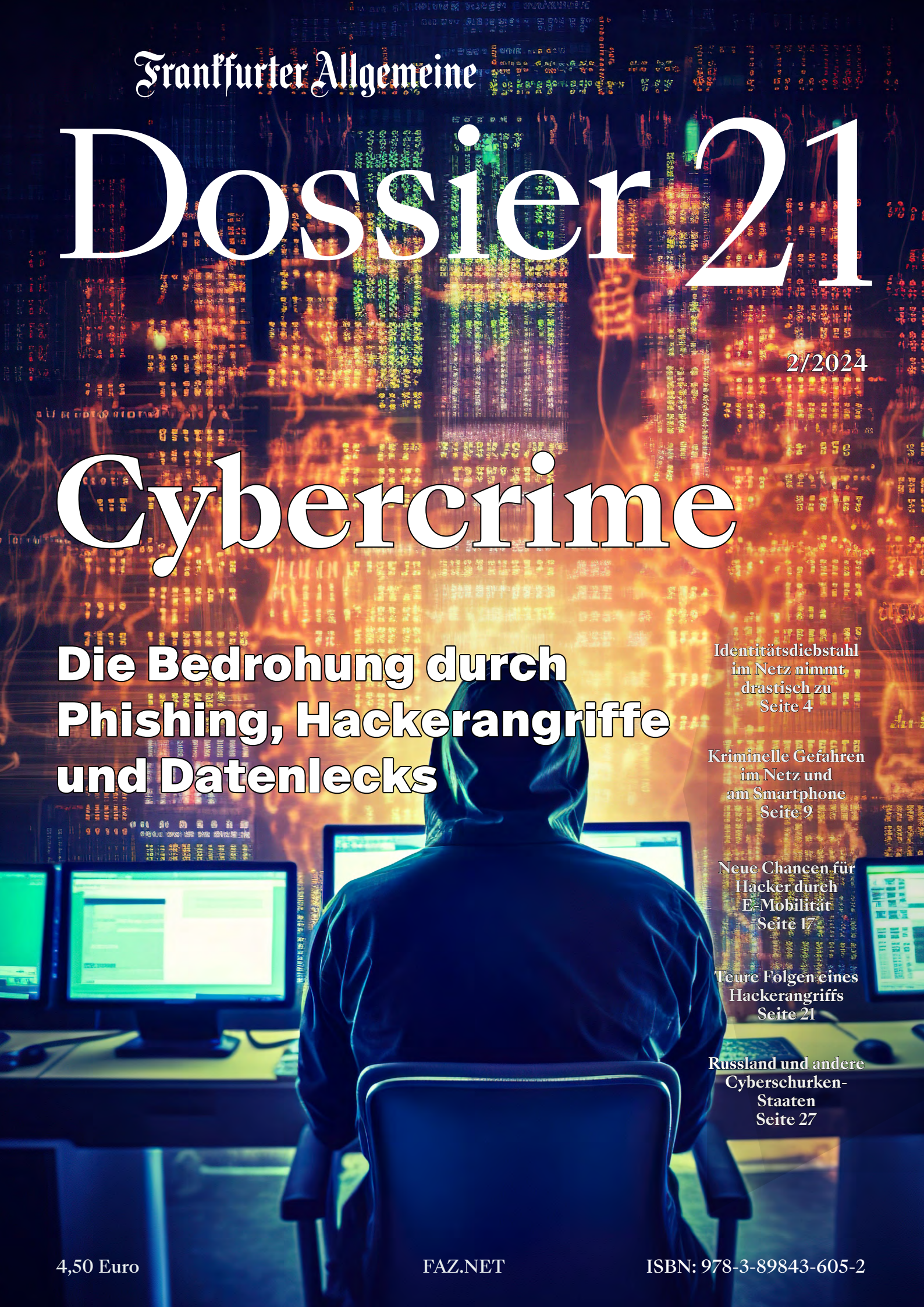
Frankfurter Allgemeine

Dossier 21

2/2024

Cybercrime

Die Bedrohung durch Phishing, Hackerangriffe und Datenlecks



4,50 Euro

FAZ.NET

ISBN: 978-3-89843-605-2

Inhalt

Impressum

Frankfurter Allgemeine Dossier
eMagazin der Frankfurter Allgemeinen Zeitung

Verantwortlich: Carsten Knop

Redaktion und Gestaltung: Birgitta Fella, Hans Peter Trötscher

Projektleitung: Olivera Kipcic (Leiterin Frankfurter Allgemeine Archiv und Rights Management)

Autoren: Holger Schmidt, Marcus Jung, Michael Spehr, Melanie Mühl, Maximilian Sachse, Stephan Finsterbusch, Monika Ganster, Friedrich Schmidt, Matthias Wyssuwa, Mona Jaeger, Piotr Heller

Titelbild und Abbildungen: adobestock.com

Produktion: F.A.Z.-Research

Anschrift: Frankfurter Allgemeine Zeitung GmbH, Pariser Straße 1, 60486 Frankfurt am Main

Geschäftsführung: Thomas Lindner (Vorsitzender), Dr. Volker Breid

Editorial

Die Bedrohung durch Cyberangriffe wächst in einer zunehmend digitalisierten Welt rasant. Identitätsdiebstahl, Phishing und Hackerangriffe sind nicht nur lästige Unannehmlichkeiten, sondern können verheerende Auswirkungen auf Individuen und Unternehmen haben. In diesem Dossier werden Aspekte der Cybersicherheit beleuchtet, um ein Verständnis der Bedrohungslage zu bieten und Möglichkeiten der Gefahrenabwehr zu zeigen.

Identitätsdiebstahl und Phishing
Identitätsdiebstahl ist eine der häufigsten und bedrohlichsten Formen der Cyberkriminalität. Fast jeder dritte Mensch in Deutschland hat bereits im privaten Umfeld Erfahrungen mit Identitätsdiebstahl gemacht.

Schwachstellen in Passwörtern
Ein weiterer kritischer Punkt sind unsichere Passwörter. Kurz und einfach zu merkende Passwörter sind ein leichtes Ziel für Hacker, die mittlerweile auch KI-basierte Werkzeuge einsetzen, um Passwörter effizient zu knacken.

Mobilität und Cybergefahren
Mit der Vernetzung von Fahrzeugen und der Integration von Softwarelösungen steigt auch das Risiko von Cyberangriffen. Dies bedeutet nicht nur eine Gefahr für die Datensicherheit, sondern auch für die physische Sicherheit der Fahrzeuginsassen dar.

Kosten der Cyberangriffe
Die finanziellen Auswirkungen eines Cyberangriffs können enorm sein. Neben Verlusten durch Diebstahl oder Lösegeldforderungen entstehen auch indirekte Kosten durch Betriebsunterbrechungen, Imageverlust und die Wiederherstellung der Systeme.

Staatlich geförderte Cyberkriminalität
Staaten wie Russland fördern Cyberkriminalität, um politische und wirtschaftliche Ziele zu verfolgen. Diese staatlich unterstützten Angriffe sind besonders schwer abzuwehren, da sie über erhebliche Ressourcen und Expertise verfügen.

Trotz der beängstigenden Bedrohungslage gibt es Hoffnung. Künstliche Intelligenz kann helfen, Bedrohungen in Echtzeit zu erkennen und abzuwehren, indem sie große Datenmengen analysiert und Muster identifiziert, die auf einen Angriff hindeuten.

Die Herausforderungen im Bereich der Cybersicherheit werden in Zukunft nicht kleiner, sondern größer. Doch mit den richtigen Technologien und Strategien können wir diesen Herausforderungen begegnen und eine sichere digitale Zukunft gestalten.

Eine spannende Lektüre wünscht
Holger Schmidt
Redaktionsleiter „Verticals und Newsletter“ FAZ.NET

Jeder Zehnte ist Opfer eines Identitätsdiebstahls geworden

Frankfurter Allgemeine Zeitung, 28.03.2024

Jeder dritte Mensch in Deutschland kennt im privaten Umfeld einen Fall von Identitätsdiebstahl. Jeder Zehnte war schon einmal direkt betroffen - und laut einer Umfrage sind junge Erwachsene besonders leichte Opfer.

Von Marcus Jung

Es sind unerklärbare Abbuchungen auf Kreditkartenkonten, Mahnungen für Onlinebestellungen oder gesperrte Zugänge für Streamingdienste: Mehr als ein Drittel der Menschen in Deutschland hat im privaten Umfeld Erfahrungen mit dem Diebstahl von Onlinekonten und der eigenen digitalen Identität gemacht, jeder Zehnte war schon direkt betroffen. Das ergab eine repräsentative Umfrage des Meinungsforschungsinstituts Yougov im Auftrag der Initiative Sicher Handeln (ISH), hinter der neben kriminalpräventiven Einrichtungen des Bundes und der Länder auch die Onlineplattform Kleinanzeigen steht.

Die hohe Zahl der Betroffenen ist kein Zufall: Die Gefahr wächst, Opfer eines digitalen Identitätsdiebstahls zu werden. Fast 185 Millionen kompromittierte Nutzerkonten zählte das Hasso-Plattner-Institut (HPI) 2021. Dazu nun eine aktuelle Einordnung: Allein im Januar dieses Jahres waren es mehr als 46 Millionen. Auf das gesamte Jahr hochgerechnet könnte sich die Zahl der Fake-Profile im Vergleich zum Jahr 2021 also fast verdreifachen.

Kriminelle nutzen KI

Die Gründer der ISH gehen davon aus, dass der zunehmende Einsatz von Künstlicher Intelligenz dazu wesentlich beiträgt. Sie erleichtert den Kriminellen die Betrugsmasche und ermöglicht es ihnen zudem, mit Skaleneffekten zu planen. "Mittels KI könnten Kriminelle ihren Betrug noch einfacher und schneller automatisieren und so zahllose Taten gleichzeitig begehen. Ein enormer Effizienzgewinn", sagt Harald Schmidt von der Stiftung Deutsches Forum für Kriminalprävention und zugleich Sprecher der Initiative.

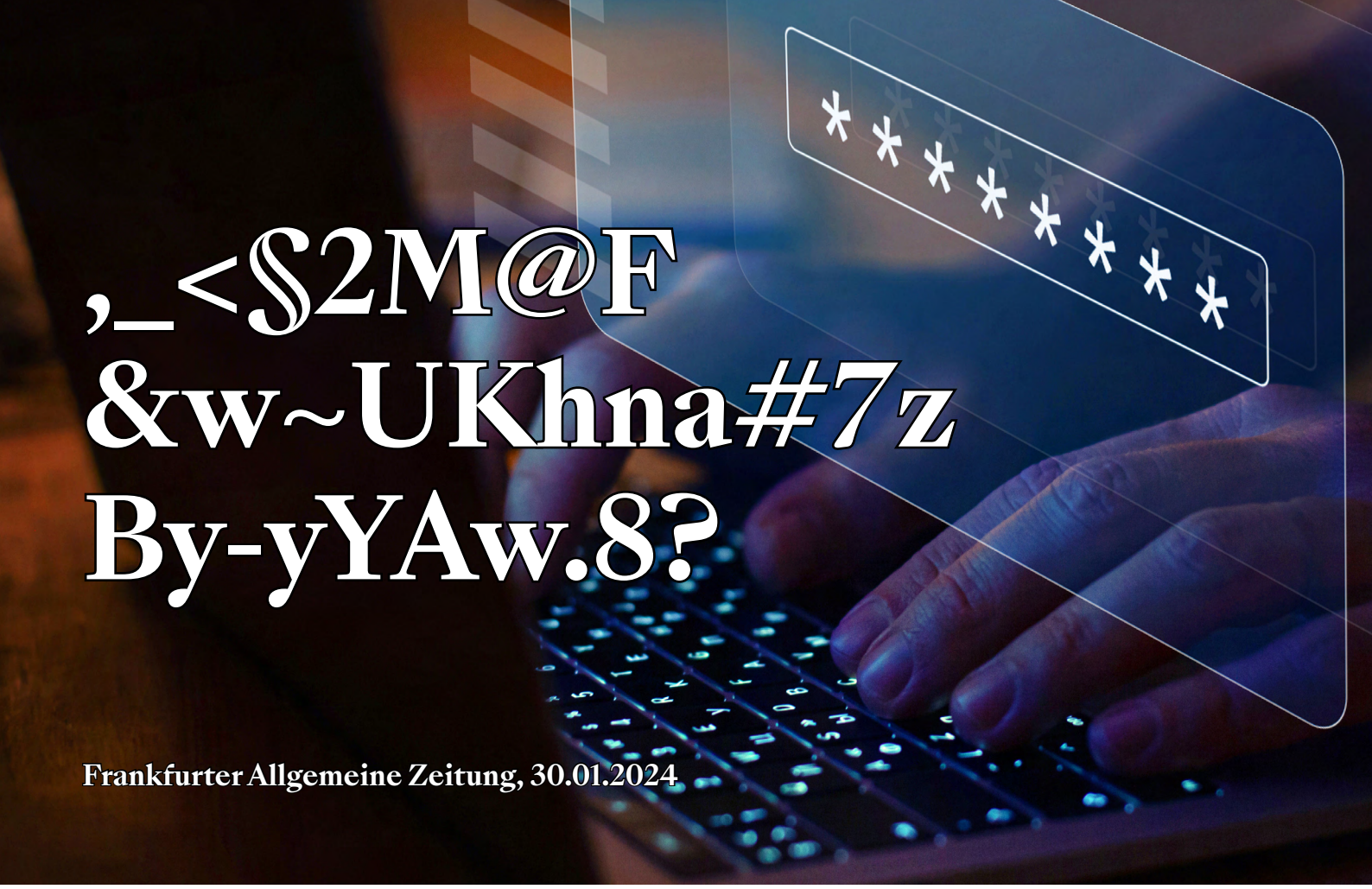
Aktuell warnt die ISH vor zwei Betrugsmaschen. Insbesondere auf den angespannten Wohnungsmärkten mehren sich Fake-Inserate, für die gestohlene Nutzerdaten verwendet werden. Damit gewinnen

die Täter das Vertrauen von Wohnungssuchenden, um abermals an Geld und Daten zu gelangen. Beim "Money Muling" bringen die Kriminellen gestohlenes Geld über die Bankkonten argloser Nutzer wieder in den Kreislauf, was den Tatbestand der Geldwäsche verwirklicht.

Jüngere sind sorgloser

Die Ergebnisse der Yougov-Umfrage zeigen außerdem, dass jüngere Menschen deutlich sorgloser mit den Risiken umgehen als ältere. Jeder dritte Umfrageteilnehmer im Alter zwischen 18 und 24 Jahren gab an, für mehrere seiner Onlinebenutzerkonten das gleiche Passwort zu verwenden. Im Durchschnitt tut dies nur jeder Fünfte (22 Prozent). Zudem bejahten 16 Prozent der "Digital Natives", schon einmal eine Kopie ihres Personalausweises an eine ihnen unbekannte Person geschickt zu haben. In der gesamten Umfrage traf dies nur auf elf Prozent zu.

Ebenjene Sorglosigkeit hatte in Deutschland zur Speicherung von Fingerabdrücken im Personalausweis geführt. Das Vorgehen hat der Europäische Gerichtshof vor wenigen Tagen für zulässig erklärt. Es sei gerechtfertigt, weil Fälschungen und Identitätsdiebstahl bekämpft werden müssten und die EU-Länder die Dokumente gegenseitig überprüfen könnten (Az. C-61/22).



’_<§2M@F &w~UKhna#7z By-yYAw.8?

Frankfurter Allgemeine Zeitung, 30.01.2024

Passwörter sollten deutlich länger werden. Die Kennwort-Knacker nutzen jetzt auch Künstliche Intelligenz.

Von Michael Spehr

Es steht schlecht um sie, und Besserung ist nicht in Sicht. Es geht um unsere Passwörter. In diesem Jahr werden Passwortknacker mit Künstlicher Intelligenz einen ungeahnten Aufschwung nehmen. Die entsprechenden Werkzeuge gibt es schon. Die KI hilft dabei, die Qualität der vorhergesagten Passwörter zu verbessern, es werden also zunächst wahrscheinliche Kennworte ausprobiert und unwahrscheinliche später. Die Tools treffen Annahmen über Kennwortmuster und verwenden Algorithmen für verkettete Kennworte.

Im vergangenen Jahr haben Sicherheitsforscher Daten aus einem Hackerangriff ausgewertet, bei dem 32 Millionen Nutzerdaten in einer unverschlüsselten Datenbank erbeutet wurden. Aus dieser Datenbank wurden alle Passwörter entfernt, die entweder sehr kurz oder länger als 18 Zeichen waren. Die verbleibenden 15,6 Millionen Passwörter wurden einer KI vorgesetzt, und nach entsprechender Auswertung hätte das entsprechende Werkzeug die Hälfte aller Kennworte in weniger als einer Minute erraten können. In weniger als einer Stunde waren es 65 Prozent, innerhalb eines Tages 71 Prozent.

Passwörter sind am unsichersten, wenn sie kurz sind und nur aus Ziffern bestehen. Sie werden um so sicherer, je länger sie sind und wenn sie aus Ziffern, Großbuchstaben, Kleinbuchstaben und Sonderzeichen bestehen. Schon durch Hinzufügen einer weiteren Komponente wächst die Sicherheit sprunghaft. Ein neunstelliges Kennwort bestehend aus Ziffern sowie Groß- und Kleinbuchstaben lässt sich in zwei Tagen raten. Lässt man ein Zeichen

Wo Cyberschurken stecken

Frankfurter Allgemeine Sonntagszeitung, 14.04.2024

Eine globale Karte der Cyberkriminalität zeigt: Die größte Gefahr geht von Russland aus. Deutschland sticht auf einem Feld hervor.

Von Piotr Heller

Vom Bruttosozialprodukt über die Alphabetisierungsquote, bis hin zur FIFA-Weltrangliste lassen sich Staaten mittels verschiedenster Kennzahlen vergleichen. Jetzt soll ein weiterer Messwert hinzukommen: der "Word Cybercrime Index", ein Maß für die Bedrohung, die von einem Land durch Cyberkriminalität ausgeht. Eine Gruppe von Wissenschaftlern hat ihn erdacht und im Magazin Plos One veröffentlicht. Der Index könnte bei der Jagd nach Cyberkriminellen helfen, weil er neben bekannten Hotspots auch Länder in den Fokus rückt, die man nicht mit Verbrechen in der digitalen Sphäre in Verbindung bringt - darunter Deutschland.

Die Forscher haben sich auf profitorientierte Cyberkriminalität fokussiert. Dazu zählen Attacken mit Erpressungssoftware, Identitätsdiebstahl und Betrugsmaschen. Zwar gibt es kaum verlässliche Zahlen über das Ausmaß dieses Problems, doch Schätzungen wie die des Branchenverbands Bitkom, der den Schaden durch Cybercrime allein in Deutschland auf über 200 Milliarden Euro im Jahr taxiert, machen klar: Das Problem ist groß. Unklar ist hingegen oft, wo die Täter stecken. Sie verschleiern ihren Standort mit technischen Mitteln, operieren über Ländergrenzen hinweg, nutzen Hardware in verschiedenen Teilen der Welt.

Mit ihrem Index wollten die Forscher Klarheit schaffen. Sie verfolgten die Spuren der Täter nicht selbst, sondern befragten 92 Cybercrime-Experten. Damit liefern sie die bislang größte derartige Untersuchung des Phänomens. Die Fachleute sollten Länder nennen, in denen sie die größten Gefahren vermuten. Daraus haben die Forscher ihren Index berechnet. Auf den Spitzenplätzen gibt es keine Überraschungen: Neben Russland finden sich dort die Ukraine und China, gefolgt von den Vereinigten Staaten, Nigeria und Rumänien.

Doch die Studie geht weiter ins Detail, denn die Experten sollten auch einzelne Feldern der Cyberkriminalität bewerten. Bei der Entwicklung von Technologien für Cyberattacken tut sich auf den ersten Rängen nichts, aber schon bei der Durchführung von Angriffen und Erpressung landet Nordkorea auf Platz drei. Was Betrugsmaschen im Internet angeht, ist Nigeria an der Spitze der Rangliste, gefolgt von den Vereinigten Staaten.

Wissenschaftler könnten den Cybercrime-Index beispielsweise mit anderen Kennzahlen wie dem Bildungsstand oder der Verfügbarkeit des Internets vergleichen, um herauszufinden, welche Faktoren diese Form der Kriminalität begünstigen, schreiben die Autoren. Ließe man dieses Wissen in Präventionsprogramme fließen, könnte man manche Fälle von Cyberkriminalität vielleicht verhindern.

Trotz solcher Ideen zeigt sich Michael Waidner, Leiter des Fraunhofer-Instituts für Sichere Informationstechnologie, von den Ergebnissen wenig beeindruckt. Er war an der Studie nicht beteiligt. Herauszufinden, welche Länder die Quelle von Cyberkriminalität seien, bezeichnet er zwar als "lohnendes Ziel", sagt aber auch: "Wenn Sie mich gefragt hätten, dann hättet ich Ihnen aus dem Bauch heraus eine ähnliche Liste genannt." Die Erkenntnisse seien nicht neu. "Ich weiß nun lediglich, dass andere Leute - die sich damit vielleicht besser auskennen als ich - ähnliche Sachen denken wie ich", erklärt er. Spannender wäre der Versuch gewesen, in die Ermittlungen zu Straftaten in den einzelnen Ländern hineinzuschauen, und daraus Schlüsse zu ziehen.

Miranda Bruce, die an der University of Oxford zu organisierter Kriminalität forscht und den Index entwickelt hat, verteidigt ihr Vorgehen. Die befragten Experten haben allesamt jahrelange Erfahrung darin, Fälle von Cyberkriminalität zu ermitteln und Täter aufzuspüren. Ihre Einschätzungen basierten auf Beweisen. "Da wir die Cyberkriminellen selbst nicht befragen können, sind diese Experten die zuverlässigste Quelle", sagt sie.

Zudem seien die Ergebnisse durchaus nicht nur erwartbar. "Ich war überrascht, dass die Experten insgesamt 97 Länder genannt haben", sagt Bruce. Das sieht Vasileios Karagiannopoulos ähnlich. Er leitet das Zentrum für Cyberkriminalität und Wirtschaftskriminalität der Universität Portsmouth und war an der Studie nicht beteiligt. "Die Länder im Mittelfeld sind besonders wichtig, weil wir über die Situation der Cyberkriminalität dort nicht viel wissen", erklärt er. Ermittlern sei klar, wo die größten Banden stecken, nur komme man gerade in Russland nicht an sie ran. Aber wenn man wisse, in welche anderen Länder die Kriminellen ihre Verbindungen pflegen, ließe sich dort ansetzen: "Die großen Fische könnten sich in einem Land verstecken, aber vielleicht müssen sie ihre Taten über Staaten lenken, wo die Behörden eher an Ermittlungen interessiert sind", erklärt der Experte.

Deutschland könnte zu diesen Ländern zählen. In der gesamten Rangliste landet die Bundesrepublik auf Platz 18 und ist in den meisten Kategorien weit hinten, außer bei der Geldwäsche. Hier findet sich Deutschland auf dem zehnten Platz. Den Grund dafür vermutet Philipp Maume, Experte für Recht der Kapitalmärkte von der TU München, in den allgemeinen Schwächen des deutschen Geldwäscherechts. "Das hat mit dem hohen Niveau des Grundrechtsschutzes zu tun, mit viel föderaler Kleinstaaterei und mit den zugleich limitierten Zugriffsmöglichkeiten der Strafverfolgungsbehörden", erklärt er.

Kryptowährungen seien hingegen nicht ausschlaggebend. Cyberkriminelle nutzen die digitalen Werte zwar für ihre Machenschaften. Jedoch weiß Maume: "Vereinfacht gesagt, waren Dienstleistungen im Kryptobereich hierzulande schon seit langer Zeit reguliert, und Deutschland ist bei den Handelsvolumina in diesem Be-

reich kein großer Player." Jedoch weist der Strafrechtler Kilian Wegner von der Europa-Universität Viadrina Frankfurt (Oder) auf mögliche Schwächen bei der Umsetzung von Regeln für Kryptowährungen hin. Nicht alle Landeskriminalämter seien fit bei Ermittlungen im Kryptobereich. "Davon profitieren Cyberkriminelle, die heute stärker denn je auf Kryptowerte setzen", sagt er.

Das Bundeskriminalamt zeigt sich interessiert an den Studienergebnissen. Carsten Meywirth, Leiter der Abteilung Cybercrime, verweist auf ein überdurchschnittlich großes Dunkelfeld. Viele Straftaten würden nicht angezeigt. "Zusätzliche wissenschaftliche Erhebungen können hier einen wertvollen Beitrag zur Aufhellung leisten und den öffentlichen Diskurs befördern", sagt er.

Das hoffen auch die Forscher. Miranda Bruce sagt, sie wisse nicht, in welche Entscheidungen ihr Index einfließen werde, fügt aber hinzu: "Die Studie und die Datensätze sind frei zugänglich, sodass jeder sie für Analysen nutzen kann."

Bald soll es auch möglich werden, Entwicklungen an den Daten abzulesen. Die ursprüngliche Umfrage unter den 92 Experten fand 2021 statt. Ende letzten Jahres haben Bruce und ihre Kollegen eine neue Befragung durchgeführt. "Damit wir untersuchen können, ob wichtige globale Ereignisse einen Einfluss auf die Lage von Cyberkriminalitäts-Hotspots haben", sagt sie. So dürfte sich bei der Analyse beispielsweise zeigen, ob der Krieg in der Ukraine die Cyberkriminalität in der Region beeinflusst. Der aktuelle Index sei bloß ein Startpunkt.