Quelle: iStock.com/thomaguery

/// CEM KARAKAYA

ist Experte für Internetkriminalität, Autor und Geschäftsführer von Blackstone432, München, www.blackstone432.de

/// DR. MARC MAISCH

ist Rechtsanwalt und Fachanwalt für IT-Recht, München, www.datenklau-hilfe.de

/// Wir werden überall beobachtet und belauscht …

SCHUTZ VOR CYBERKRIMINALITÄT

CEM KARAKAYA / MARC MAISCH /// Wir surfen uns durch die Welt, posten mehr oder weniger Privates in den Sozialen Medien, machen Überweisungen nur noch via Online-Banking. Vieles hat sich ins Netz verlagert. Doch wie sicher bewegen wir uns im Internet? Gehen wir zu sorglos um mit unseren Daten im Netz? Der Experte für Internetkriminalität Cem Karakaya entführt uns ins Darknet der Cyberkriminellen und verrät gemeinsam mit Marc Maisch, Rechtsanwalt für IT-Recht und Datenschutz, hilfreiche Tipps, um sicher online zu sein.

Politische Studien: Cyberkriminalist, Cyberagent. Sind Sie ein James Bond des World Wide Web und des Darknets, Herr Karakaya?

Cem Karakaya: (lacht) So könnte man das sagen. Wie James Bond, aber ohne schöne Frauen und schöne Autos. (lacht) Ernsthaft: Unser Grundauftrag ist es, die Menschen zu sensibilisieren und zu informieren, welche Gefahren im Netz lauern. Denn nur derjenige kann sich schützen, der die Gefahr kennt. Doch um gleich die Erwartungen zu dämpfen: Bei der Internetkriminalität hat die Polizei wenig Chancen, da wir kein Tatortprinzip haben. Unser Opfer sitzt in Deutschland, der Server steht in China und der Täter hält sich in Russland auf. Da wird es schwierig für die Polizei. Umso wichtiger ist es, dass wir mittels Vorträgen präventiv schulen und sensibilisieren.

Leider nimmt die Kriminalität im Internet zu. 2020 wurden in Deutschland 61 Prozent der Internetnutzer Opfer von Cyberkriminalität. Das sind sechs von zehn Usern und im Vergleich zum Vorjahr ein beachtlicher Anstieg von 6 Prozent. Woran liegt das?

Das überrascht mich überhaupt nicht. Es überrascht mich eher, dass es so wenig sind. Die Menschen sind viel zu leichtsinnig. Die erste Frage dazu ist: Wie sieht es mit der Sicherheit der eigenen technischen Geräte aus? Sind beispielsweise beim WLAN-Router zu Hause aktuelle Sicherheitsupdates drauf? Wurde das WLAN-Passwort geändert oder gilt noch das, was hinten auf dem Gerät steht? Viele Menschen ändern das nicht, was ein großer Fehler ist. Wie viele Gäste kennen bei Ihnen zu Hause bereits Ihr WLAN-Passwort? Wenn ich bei Ihnen zu Hause Gast wäre und Sie mir Ihr Passwort geben, kann ich von hundert Metern Entfernung, also von außerhalb und je nach Signalstärke, böswillige Aktionen starten, die Sie überhaupt nicht mitbekommen. Die Menschen nehmen sich leider für die Sicherheit ihrer Geräte keine Zeit. So wird es den Kriminellen auch leichtgemacht.

Lassen Sie uns das mehr sortieren. Welche Art von Cyberangriffen gibt es denn überhaupt? Und welche sind die größten Gefahren für Privatleute?

Wenn Sie alle Cyberangriffe zusammenfassen, fangen bis zu 80 Prozent aller Angriffe mit einer sogenannten

> Die Menschen nehmen sich für die **SICHERHEIT** ihrer Geräte keine Zeit.

> Der zweitgrößte Cyberangriff läuft über **VERSEUCHTE** Internetseiten, die im Hintergrund den Computer infizieren.

Phishing-E-Mail an. Ich bekomme angeblich von meiner Bank eine E-Mail, weil etwas mit meinem Konto nicht stimmt und werde aufgefordert, auf einen bestimmten Link zu klicken. Folge ich der Aufforderung, lande ich auf einer gefälschten Online-Banking-Seite, die wie eine echte aussieht. Gebe ich dort meine Daten ein sind sie „abgefischt". Dieses Problem haben wir nicht nur im Online-Banking-Bereich, sondern auch bei den sozialen Netzwerken, auf Shopping-Seiten etc. Daher empfehlen wir, unbedingt die Zwei-Faktor-Authentifizierung (ZFA) zu aktivieren. Das bedeutet, dass ich einen bestimmten Code per SMS bekomme. Das wiederum heißt: Selbst, wenn die Täter im Besitz meiner Zugangsdaten sind, haben sie trotzdem nicht die Möglichkeit, sich ohne diesen Code bei mir anzumelden. Die abgefischten Daten sind für die Täter somit nutzlos.

Marc Maisch: Auch im Bereich Online-Banking wird die ZFA benutzt. Ich selbst mache Online-Banking mit einem TAN-Generator. In dem Fall ist mein TAN-Generator der zweite Faktor, weil das Gerät weder mit meinem Computer noch mit meinem Internet eine Verbindung hat. Mein Bildschirm zeigt ein blinkendes Zeichen und mein TAN-Generator muss das Auslesen. Danach stellt mir der Generator diese zwei Fragen: „Stimmen die Kontonummern überein?" und „Stimmt der Betrag?". Wenn ich diese sieben Sekunden Zeit investiere und tatsächlich kontrolliere, ob die Daten übereinstimmen, ist Online-Banking absolut sicher.

Leider haben wir laufend neue Fälle, in denen Betroffene die Kontrolle über ihre Bankkonten aus der Hand geben oder Gelder direkt an Kriminelle überweisen. Bei einer sorgfältigen Überprüfung der Bankdaten hätte man aber leicht feststellen können, dass die Daten nicht übereinstimmen, und den Vorgang abbrechen können. Wenn man diese Betroffenen nun fragen würde, ob Online-Banking sicher ist, würden sie sicher sagen: „Nein, ist es nicht." Hier stellt sich nun die Frage: Ist jetzt die Technologie daran schuld oder der Mensch, der sie benutzt (und reingelegt wird)?

Also unbedingt die Zwei-Faktor-Authentifizierung nutzen. Wie schlagen Cyberkriminelle noch zu?

Cem Karakaya: Der zweitgrößte Cyberangriff läuft über verseuchte Internetseiten, die im Hintergrund versuchen, meinen Computer zu infizieren. Meist passiert dies beim Auf-

ruf erotischer Seiten, die sehr viele Menschen benutzen ... (lacht) Das betrifft aber auch illegale Streaming-Seiten, auf denen Menschen einen aktuellen Kinofilm oder Serien anschauen, ohne einen Cent dafür zu bezahlen. Hier sind die blinkenden Werbebanner das Problem. Hinter diesen läuft nämlich ein so genanntes Skript, welches im Hintergrund überprüft, ob Sie die richtigen sicheren Maßnahmen getroffen haben. Wenn nicht, ist der Trojaner drauf, ohne dass Sie es mitbekommen.

Man kann diese Werbung doch auch abstellen ...

Ja, natürlich. Dann können Sie aber auch keinen Film oder keine Serie mehr anschauen und auf der Seite kann man nur noch Text lesen. Es gibt kein Bild und auch kein Video mehr. Die Lösung dafür wäre, dass man ein aktuelles Anti-Virus-Programm (End Point Security) mit einer Firewall benutzt. Damit kann der Netzwerkverkehr kontrolliert werden. Wenn jemand versucht, mit

Im Internet bezahlen wir mit unseren Daten, warnt Cem Karakaya aus seiner jahrelangen Erfahrung mit Kriminalität im Netz heraus.

Quelle: HSS, Monika Zeitler

> Ich würde **NIEMALS** auf einer Seite aktiv werden, wenn die Verbindung nicht verschlüsselt ist.

meinem Computer eine verdächtige Verbindung aufzubauen, warnt mich meine Firewall. Viele solcher Seiten sind bereits bekannt, deshalb raten die Anti-Virus-Programme dann von dem Besuch dieser ab.

Und wer kann mir bei den korrekten sicheren Einstellungen helfen?

Ich zum Beispiel ... (lacht) Zu diesem Thema halte ich immer wieder Vorträge. Aber es existieren auch im Internet viele gute Seiten, auf denen Informationen rund um sicheres Surfen stehen. Man muss und sollte für seine Sicherheit Zeit und Geld investieren.

Warum investieren wir denn nicht in unsere Sicherheit?

Weil wir daran gewöhnt sind, immer alles kostenlos zu erhalten. Wenn ich aber nicht mit Geld bezahle, bezahle ich mit meinen sehr wertvollen persönlichen Daten. Wenn Sie für ein Produkt nichts bezahlen, sind Sie das Produkt.

Es gibt noch andere typische Fallen im Privatleben. Also wenn ich zum Beispiel eine Reise mache ... und im Hotel WLAN nutze.

Es beginnt schon viel früher. Sie möchten eine Reise im Internet buchen. Aber es gibt sehr viele gefälschte Reisebuchungsseiten dort. Jetzt stellen Sie sich einmal vor: Sie buchen und bezahlen eine Reise. Sie denken, es sei alles reserviert und in Ordnung. Sie kommen dann ins Hotel – und es heißt: Es gibt keine Reservierung unter Ihrem Namen und es ist auch nichts bezahlt worden. Dieser Falle kann ich entgehen, wenn ich ein paar Anzeichen, wie ich zwischen gefälschten und richtigen Internetseiten unterscheiden kann, beachte.

Zum einen fangen viele gefälschte Seiten mit „http://...“ an und nicht mit „https://....“. Der Buchstabe „s“ steht für eine sichere und verschlüsselte Verbindung. Ich würde niemals auf einer Seite aktiv werden, wenn die Verbindung nicht verschlüsselt ist. Zum anderen haben viele gefälschte Seiten weder ein Impressum noch eine Datenschutzerklärung. Beides sollte aber auf jeden Fall vorhanden sein. Und ein dritter Hinweis lautet: Wenn ein Smartphone, das normalerweise 1.000 Euro kostet, für 250 Euro angeboten wird, ist dies ein eindeutiges Zeichen dafür, dass ich mich auf einer betrügerischen Seite befinde. Also auch bitte stets mit gesundem Menschenverstand einkaufen.

Zurück zu unserem Urlaubstraum: Wenn alles korrekt war und ich im Hotel sitze …

… dann wollen Sie das hoteleigene WLAN nutzen. Manche Hotels haben nicht einmal ein Passwort, was sehr gefährlich ist. Wenn sich ein Hacker oder Krimineller ebenfalls in diesem Hotel befindet, könnte er über denselben WLAN-Router direkt in Ihr Gerät hineinschauen. Er sieht alles, was in Ihrem Gerät ist, und was Sie mit Ihrem Smartphone oder Computer machen. Dagegen kann man sich mit so genannten Virtual Private Network (VPN)-Diensten schützen. Ich benutze zum Beispiel eine extra Sicherheits-App, die mein VPN einschaltet. Damit wird die Verbindung verschlüsselt. Somit kann niemand aus demselben Netzwerk auf meine Geräte zugreifen. Generell benutze ich immer meine eigene Internetverbindung. Muss ich dann doch mal auf das hoteleigene WLAN zugreifen, aktiviere ich die VPN-App.

Was haben Sie noch auf Ihrem Handy installiert?

Ich habe zusätzlich das Passwort-Manager-Programm meines Anti-Virus-Programmes installiert, damit ich unterschiedliche Passwörter verwalten kann. Darüber hinaus nutze ich Fotosafe. Das ist eine App, auf der Fotos gespeichert sind, und auf die andere Apps keinen Zugriff haben. Und ich habe die Family-App. Damit kann ich sehen, was meine Tochter auf ihrem Smartphone macht. Ich habe ihr das gezeigt und erklärt, dass mein Ziel nicht ist, sie zu überwachen, sondern sie zu begleiten. Dies ist mein Auftrag als Vater. Wenn ich feststelle, dass sie in eine falsche Richtung geht, warne ich sie und erkläre, warum diese Richtung falsch ist. Ich habe ihr auch gesagt, dass sie alles sehen kann, was ich mit meinem Smartphone mache. Dann war sie damit einverstanden. Was sie nicht weiß, ist, dass ich ein zweites Smartphone habe. (Beide lachen)

Gehen wir noch einmal zurück. Wenn ich bemerke, dass ich betroffen bin: Wie soll ich mich verhalten?

Sie müssen unbedingt bei der Polizei Anzeige erstatten, auch wenn diese nicht jeden Täter finden kann. Aber der Fall muss bei der Polizei gemeldet werden. Wenn später nämlich ein Identitätsdiebstahl passiert, kann man sagen, dass man damals schon etwas bemerkte, und auf seine Anzeige verweisen. Ich habe somit ein Beweismittel in der Hand, dass ich bereits bei der Polizei war. Selbst wenn

> Hauptsache ist, dass man überhaupt ein **ANTI-VIRUS-PROGRAMM** installiert hat.

ein Fall von der Staatsanwaltschaft eingestellt wurde, gibt es ein Aktenzeichen, das beweist, dass ich Anzeige erstattet hatte.

Was kann die Polizei gegen Cyberkriminelle unternehmen?

Die deutsche Polizei führt seit acht bis zehn Jahren ein Cybercrime-Dezernat. Wir haben in München etwa 120 bis 130 Kollegen, die in Sachen Cybercrime ermitteln. Jeder von ihnen erhält am Tag bis zu 30 Fälle. Alle müssen bearbeitet, Vernehmungen durchgeführt, Beweise gesammelt werden, die Staatsanwaltschaft muss alles vorbereiten. Die etwa neun Staatsanwälte bekommen wiederum 700 bis 800 Fälle pro Tag auf den Tisch. Jetzt können Sie sich das Ausmaß vorstellen.

Du meine Güte …

Genau. Deswegen benötigen wir auch hier gut ausgebildetes Personal, das sich mit der Materie bestens auskennt. In Bayern wurde deshalb das Cypercop-Programm aufgelegt, bei dem Experten aus den Bereichen IT und Wirtschaft zusammengebracht werden.

Das klingt gut. Denn wir wollen es ja den Hackern schwermachen. Wie kann ich das schaffen? Wie kann ich mich wirklich gut schützen?

Das können nur die Menschen selbst schaffen. Ich sage immer: „Der Computer rechnet mit allem, aber nicht mit seinen Benutzern." Wenn die Menschen sich Zeit nehmen, Aktualisierungen sofort und nicht später durchführen und für ihre Sicherheit Geld investieren, ist schon viel geholfen. Dazu gehört ein aktuelles und den Bedürfnissen entsprechend eingestelltes Anti-Virus-Programm sowie sich immer im Internet in Sachen Cybersicherheit zu informieren, zum Beispiel beim Bundesamt für Sicherheit in der Informationstechnik (BSI), auf der es eine Seite für Bürger gibt. Das BSI verschickt alle zwei bis drei Wochen einen Newsletter über die aktuellsten Gefahren (https://www.bsi.bund.de). Und es gibt noch zwei sehr empfehlenswerte Internetseiten darüber, wie man als Eltern Kindern Medienkompetenz beibringt: klicksafe.de oder schau-hin.info. Das Problem ist nur, dass Kinder eher den Eltern etwas beibringen können als umgekehrt. Eltern können ihre Kinder oftmals nicht begleiten, weil sie sich zu wenig auskennen.

Quelle: HSS, Monika Zeitler

Kann man angesichts der vielen Gefahren überhaupt noch sicher im Internet kommunizieren, fragt sich auch Susanne Hornberger, Leiterin Kommunikation und Öffentlichkeitsarbeit der Hanns-Seidel-Stiftung, im Gespräch mit den Fachleuten.

Das ist leider so. Gibt es ein empfehlenswertes Anti-Virus-Programm?

Welches, ist egal. Hauptsache ist, dass man überhaupt ein Anti-Virus-Programm installiert hat. Die Täter bemerken das Programm sofort und ziehen weiter. Sie wollen ja ein leichtes Opfer. Das ist wie bei einem Einbrecher: Er versucht einzubrechen, was durchschnittlich 12 oder 13 Sekunden dauert. Stellt er fest, dass es nicht funktioniert, weil Maßnahmen dagegen getroffen wurden, kommt das nächste Fenster an die Reihe. Dasselbe gilt übrigens auch für Trojaner, Viren und Co. Sie überprüfen ebenfalls, ob sie schnell ins System hineinkommen. Funktioniert das nicht, machen sie sich auf zum nächsten System. Es sind ja noch Trillionen von Systemen vorhanden.

Sie haben es vorhin schon angedeutet: Passwörter sind extrem wichtig.

Ja, sehr wichtig.

Was beinhaltet ein wirklich sicheres Passwort? Und wie oft muss ich das ändern, um safe zu sein?

Wenn ich ein sicheres System habe und überall unterschiedliche Passwörter benütze, dann muss ich im Grunde genommen auch meine Passwörter nicht ändern. Aber ich empfehle immer die Verwendung von

Passwort-Manager-Programmen. Ich gebe überall dasselbe Passwort ein und das Programm vergibt für mich überall unterschiedliche Passwörter. Und diese werden verschlüsselt auf meinem Container auf der Festplatte gespeichert. Auch diese Passwörter könnte man knacken, aber das dauert bis zu 140 Jahre.

Sollte man kein Passwort-Manager-Programm nutzen, rate ich dringend dazu, unterschiedliche Passwörter zu nutzen. Man kann selbst eine Methode entwickeln, beispielsweise mit einem Hauptwort „Leberkäsesemmel". Danach nehme ich von jeder Plattform die ersten und die letzten zwei Buchstaben: für Facebook zum Beispiel „Fa" und „ok". Mein Passwort für Facebook lautet somit: FaLeberkäsesemmelok.

Jetzt könnte ich noch Buchstaben mit Zahlen ersetzen: „O" schaut wie eine Null aus, „E" wie drei, „A" wie vier, „S" wie fünf und so weiter. F4L3b3rkä5353mm3l0k wäre das Passwort für mein Facebook-Konto.

Da stellt man sich aber schon die Frage: Ist es überhaupt sicher, im Internet zu kommunizieren?

Natürlich ... wenn ich verschlüsselt kommuniziere. Bei WhatsApp beispielsweise sind die Nachrichten Ende-zu-Ende verschlüsselt. Die Metadaten, also wer hat wann, wem, wohin etwas geschickt, jedoch nicht. Die Alternativen wie Signal oder Telegram verschlüsseln auch die Metadaten. Wir könnten zum Beispiel über Signal verschlüsselt telefonieren, nicht einmal der Staat kann hierbei mithören.

Auch per E-Mail gibt es eine Methode, mit der ich meine Nachricht zum Beispiel an meinen Rechtsanwalt verschlüssele. Nur er kann das dann lesen, weil sich der Schlüssel in seinem Rechner befindet. Wenn ich eine E-Mail unverschlüsselt verschicke, ist das wie bei einer Postkarte, die ich ohne Umschlag versende. Zertifikatsfirmen bieten E-Mail-Verschlüsselung an. Ich nutze PGP – Pretty Good Privacy. Man lädt sich ein Zertifikat herunter, womit ich einen öffentlichen und einen privaten Schlüssel erhalte. Den Privatschlüssel auf meinem Rechner darf niemand kennen. Den öffentlichen Schlüssel lade ich auf deren Server hoch.

Das klingt spannend, aber doch kompliziert. Und immer mehr Menschen wollen alles vereinfacht haben. Deshalb wird auch das SmartHome, also das digitalisierte Heim, immer beliebter. Was sagen Sie dazu in puncto Sicherheit?

> Wenn ich eine E-Mail **UNVERSCHLÜSSELT** verschicke, ist das wie bei einer Postkarte, die ich ohne Umschlag versende.

Es gibt nie eine hundertprozentige Sicherheit, wenn irgendetwas mit einem Netzwerk internetverbunden ist. Es gibt keine einzige Firma, die im Bereich SmartHome schriftlich absolute Sicherheit anbietet. Fragt sich dann, warum gehen wir dennoch dieses Risiko ein? Man hat zum Beispiel mit Hilfe einer Barbiepuppe ein komplettes Haus unter Kontrolle genommen, weil die Puppe mit dem WLAN-Router verbunden war ...

Die Barbiepuppe?

Ja, die Eltern hatten eine Barbiepuppe gekauft, damit das Kind mit ihr sprechen kann – so wie mit Siri. Jedenfalls sind die Täter über die Barbiepuppe in den WLAN-Router reingekommen, und damit waren sie im Haus und in jedem Gerät.

Das klingt gruselig. Lassen Sie uns einen Blick auf Unternehmen werfen, die immer wieder gehackt werden. Woran liegt das?

Ich kann Ihnen drei Beispiele nennen, die wir in der vergangenen Zeit hatten. Erster Fall: Eine Firma ruft bei uns an und sagt: „Wir haben einen Trojaner. Bitte kommen Sie und säubern Sie das System." Unser Team geht hin und stellt fest: Die Firma hat diesen Trojaner bereits seit 16 Jahren. Von 38 Rechnern sind 37 betroffen. Der Trojaner hat sich gut versteckt. Da die anderen Rechner sich im selben Netzwerk befinden, waren auch sie betroffen – bis auf einen Rechner, der mit dem Netzwerk nicht verbunden war.

Zweiter Fall: Eine Firma ruft an und klagt über Probleme. Unser Team stellt fest, dass die Firma als Betriebssystem noch immer Windows 98 installiert hat. Schon Windows 7 wird heutzutage nicht mehr aktualisiert. Als ich mit dem Chef deswegen telefoniere, erklärt er mir, dass er jedes einzelne Laborgerät entsorgen müsste, würde er das Computer-Betriebssystem aktualisieren, da diese nicht mit höheren Betriebssystemen arbeiten können.

Dritter Fall: Der Administrator einer Firma, der entlassen wurde, stellt fest, dass man sein Admin-Passwort nicht geändert hat. Was macht er? Er verbindet sich und benutzt die Leistung der Serveranlage seiner ehemaligen Firma für sein Bitcoin-Mining. Wenn man einen Arbeitnehmer entlässt, sollte man auch so schnell wie möglich dessen Zugangsdaten deaktivieren oder ändern.

Lassen Sie mich raten: Das machen viele Firmen wohl nicht?

> Mit dem **PEN-TEST** kann man die IT-Sicherheit testen.

Genau. Die Gefahr gibt es aber auch im privaten Bereich. Man befindet sich zum Beispiel in einer Beziehung und derjenige, der sich mit IT gut auskennt, richtet alles ein: WLAN-Router, soziale Netzwerke, Smartphones etc. Dann geht die Verbindung in die Brüche. Der „Experte" kauft sich ein zweites Smartphone, meldet sich mit den Zugangsdaten des anderen an und hat sofort ein Klon-Smartphone des Ex-Partners in der Hand. Ab sofort kann er jede Nachricht lesen, den Gesprächen lauschen, dank der „Mein-Gerät-Suche" den anderen sofort orten etc. Oder er geht in die E-Mail-Einstellungen und aktiviert die Umleitung zur eigenen E-Mail-Adresse. Ab sofort kann er jede E-Mail filtern ...

Das ist furchtbar ...

... und keine Seltenheit. Ich bekomme sehr viele Hilferufe von Frauen, die sagen, dass ihr Ex-Partner sie gehackt habe. Ich sage ihnen: „Nein, hat er nicht." Und frage sie: „Haben Sie nach der Trennung Ihre Zugangsdaten, Passwörter, PIN-Nummern, WLAN-Passwort geändert?" Das ist meistens nicht der Fall. Man denkt an so etwas meist nicht, wie die Verantwortlichen in Firmen eben auch.

Dazu ein Beispiel: Eine Firma testet ihre IT-Sicherheit mittels PEN-Test. Das funktioniert so: Üblicherweise schickt ein Krimineller, der vorgibt, für diese Firma zu arbeiten, an die Mitarbeiter eine E-Mail mit der Aufforderung, so schnell wie möglich die Passwörter zu ändern. Gleichzeitig schickt er einen Link mit. Wer diesen anklickt und glaubt, dass er damit sein Passwort ändert, hat eigentlich seine Zugangsdaten bekannt gegeben. Aber beim PEN-Test passiert dies nicht wirklich, sondern die Mitarbeiter bekommen ein Warn-Video angezeigt, in welchem erklärt wird, dass man gerade einen Fehler gemacht hat und für die Zukunft aufpassen soll. Aber nicht alle verstehen diesen Test und die Warnung. Ein Mitarbeiter schickte zum Beispiel diese E-Mail zurück: „Ich würde ja gern mein Passwort ändern, aber es kommt ständig das blöde Video." (Kopfschütteln)

Welche Tricks der Cyberkriminellen gibt es noch?

Zum Beispiel Ransomware – Verschlüsselungstrojaner. Dabei werden die Daten verschlüsselt und das Programm, also nicht die Täter, schickt automatisch an eine Firma solch eine E-Mail: „Wir haben Ihre Daten verschlüsselt. Ab jetzt haben sie 48 Stunden Zeit. Entweder Sie bezahlen den Betrag oder Sie können Ihre Daten

vergessen.“ Das Programm zählt automatisch runter, bei Null kann nicht mal der Hacker die Daten retten. Das kann passieren, wenn man einen falschen Anhang öffnet. Die beste Maßnahme dagegen ist ein Backup, also eine Datensicherung, die auf jeden Fall getestet werden muss, ob sie auch funktioniert hat.

Neben der IT-Sicherheit einer Firma ist es aber auch unerlässlich, die Mitarbeiter dafür zu sensibilisieren. Ich kann Millionen Euro in meine IT-Sicherheit investieren, aber das nützt nichts, wenn die Mitarbeiter die Gefahren nicht kennen. Sicherheit ist nur mit einem Team und im Team möglich. Dies gilt auch für den privaten Bereich. Zwischen November 2019 und Februar 2020 wurden beispielsweise Besucher erotischer Seiten mit der E-Mail-Masche erpresst und diese haben den Tätern 500.000 Dollar überwiesen. Die Täter selber mussten fast nichts dafür machen. Das E-Mail-System hat selbsttätig gearbeitet, und zwar so klug, dass sich die E-Mails in Deutschland bereits automatisch in deutsche Sprache übersetzt haben.

Das ist ziemlich unfassbar. Aber wie Sie vorhin bereits betont haben, das Problem ist der Mensch.

Menschen sind oft sehr naiv und gutgläubig. Oder meinen Sie wirklich, dass WhatsApp Milliarden Dollar investiert, nur damit wir untereinander kostenlos Text- und Sprachnachrichten verschicken können? Wir bezahlen mit unseren wertvollen persönlichen Daten. Deshalb tun mir auch die heutigen Kinder und Jugendlichen leid. Sie sind die erste Generation, über die man von Anfang an Daten sammelt. Und sie sind die zukünftigen Entscheidungsträger, Politiker, Staatsanwälte, Anwälte und Richter. Wenn ich bereits heute so viele Daten und Informationen über sie habe, dann habe ich in der Zukunft zwei Waffen gegen sie, nämlich sie zu manipulieren und im schlimmsten Fall zu erpressen.

Man darf nicht vergessen: einmal im Internet, immer im Internet. Es gibt heute zum Beispiel schon sehr viele Firmen, die Bewerbungsunterlagen nicht mal mehr durchlesen. Sie nehmen nur Namen, Anschrift und Geburtsdatum und recherchieren dazu im Netz. Und das spuckt eine Menge Daten aus. Und dann wird entschieden: Stelle ich die Person ein oder nicht?

Stichwort Kinder. Die meisten haben mit zehn Jahren bereits ein Smartphone.

> Ich kann Millionen Euro in meine IT-Sicherheit investieren, aber das nützt nichts, wenn die **MITARBEITER** die Gefahren nicht kennen.

Das World Wide Web ist Segen und Fluch zugleich. Über die Gefahren im Netz und wie man sich davor schützen kann, spricht Susanne Hornberger mit dem Fachanwalt Marc Maisch (m.) und dem Fachmann für Cyberkriminalität, Cem Karakaya (r.).

Ein Smartphone ist für Kinder absolut nicht geeignet. Wenn heute jemand über Kinder- und Jugendschutz spricht, muss ich lachen. Den gibt es doch heute gar nicht mehr. Früher gab es in Videotheken zum Beispiel einen Bereich, der erst ab 18 Jahren zugänglich war. Heute bekommen Kinder das Smartphone ihrer Eltern ausgehändigt und müssen lediglich in der Suchmaschine „Porno" eingeben.

Da geht es vor allem um Medienkompetenz. Sollte dies nicht endlich ein Schulfach werden?

Jein. Ich sage immer, die Hauptaufgabe liegt bei den Eltern. Die Schule kann nur unterstützen. Die rechtlichen Grenzen kann die Polizei erörtern. Wir sind deshalb auch in den Schulen unterwegs und versuchen, die Kinder zu sensibilisieren. Allerdings denken viele Erwachsene, das Internet sei ein rechtsfreier Raum. Mit dieser Einstellung liegen sie aber gänzlich falsch. Jeder Straftatsbestand, den ich im Strafgesetzbuch finde, gilt auch für das Internet. Auch in Nachrichtendiensten wie WhatsApp ist Beleidigung, Erpressung oder Morddrohung ein Straftatbestand. All das kann angezeigt werden. Auch meine zivilrechtlichen Möglichkeiten wie Unterlassungsforderung, Kontaktverbot oder Platzverweis, was insbesondere in den Schulen wichtig ist, kann ich hier nutzen.

Was ist denn beim Thema Cybermobbing wichtig?

> Jeder Straftatsbestand, den ich im Strafgesetzbuch finde, gilt auch für das **INTERNET**.

Hier gibt es durchaus rechtliche Möglichkeiten. Wichtig ist, dass man selbstbewusst ist, für seine Rechte kämpft und zeigt, dass man kein Opfer ist. Dieses Selbstbewusstsein ist äußerst wichtig. Dazu gehört, dass Eltern Kinder dabei unterstützen, eigene Entscheidungen zu treffen. Das Allerwichtigste sind Prävention und Vertrauen sowie eine gute und offene Kommunikation zwischen Eltern und Kindern.

À propos Kommunikation. Fake News und DeepFake greifen in beängstigender Schnelligkeit um sich.

Ja, das ist tatsächlich ein großes Problem. Fake News verbreiten sich so schnell, weil sie aufregend sind. Die Wahrheit ist vielen wohl zu langweilig. Und DeepFake, also Videos mit gefälschtem, also montiertem Inhalt, greift auch immer mehr um sich. Es ist schon gefährlich, wenn beispielsweise die Rede des US-Präsidenten videotechnisch manipuliert wird.

Können Sie als Experte DeepFake entdecken?

Cem Karakaya: Dafür gibt es technische Möglichkeiten und Programme, die aber in der Regel kein Mensch zu Hause installiert hat.

Marc Maisch: Das Problem ist auch, dass Menschen wirklich glauben, man könne sich auf den Social-Media-Kanälen informieren. Sie vertrauen Facebook und gehen davon aus, dass die Informationen dort redaktionell überprüft werden. Dabei ist dort ganz oft nur der Unsinn zu finden, den andere Leute verbreiten.

Cem Karakaya: Die Hanns-Seidel-Stiftung führt sehr gute Projekte und Seminare zum Thema „Erkennen von Fake News“ durch. In den Schulen beispielsweise sollte auch darüber gesprochen werden, dass auf YouTube etwa 30 Prozent aller Videos gefälscht sind, bei TikTok sind es gar 40 Prozent aller Videos. Kinder können erst ab 16 Jahren medizinisch betrachtet hundertprozentig zwischen Realität und Fake unterscheiden.

Marc Maisch: Wir beobachten ebenfalls, dass immer mehr Menschen die Fähigkeit verlieren zu googeln, also Sachverhalte kritisch zu hinterfragen und zu recherchieren, so zum Beispiel bei der Frage „Ist der Internetshop XYZ ein Fake?“ oder „Welche Erfahrungen gibt es mit XZY?“. Man sollte bei Google den Namen plus

„Abzocke“ eingeben und schon erhält man wichtige Ergebnisse, wie zum Beispiel Posts von Menschen, die mit diesem Internetshop schlechte Erfahrungen gemacht haben.

Cem Karakaya: Für diese Recherche benötigt man nur eine Minute – und das würde absolut helfen.

Marc Maisch: Richtig. Ich habe Mandanten, denen 100.000 Euro vom Online-Bankkonto abgebucht wurden, weil sie auf Betrüger hereingefallen sind. Das beginnt meistens auf Social Media mit einer Fake-Werbung mit einem angeblich prominenten Unterstützer.

Herr Dr. Maisch, Sie sind Datenschutzexperte und haben immer wieder mit Menschen zu tun, denen ihre eigene Identität gestohlen wurde. Wie oft passiert so etwas?

Marc Maisch: Ununterbrochen. Identitätsdiebstahl passiert folgendermaßen: Wenn ich Vorname, Nachname und Geburtsdatum einer Person weiß, kann ich mit dieser Identität im Internet einkaufen gehen. Sie können so überall auf Rechnung etwas bestellen. Die Firma checkt kurz, ob es diese Person gibt, indem sie eine Anfrage bei der Schufa stellt, was etwa eine Mikrosekunde dauert. Und die Schufa meldet zurück, dass sich in ihrem Datensatz eine Person mit diesem Datensatz befindet und diese Person Bonität hat, also wahrscheinlich bezahlen wird. Das genügt, um auszuliefern. Wird nicht bezahlt, meldet sich die Inkassofirma. Antwortet der Betroffene nicht, folgt ein Mahnbescheid, später ergeht vielleicht sogar ein Haftbefehl oder ein Konto wird gepfändet. Der Sog kann weitergehen: Plötzlich kann er Leasingraten des Autos oder den Hauskredit nicht mehr bezahlen. Das heißt im Umkehrschluss: Ein Opfer von Identitätsdiebstahl muss schnellstens reagieren, es muss sofort zum Anwalt gehen und Strafanzeige erstatten.

Welche Chancen hat der Betroffene?

Identitätsdiebstahl ist strafbar, zum Beispiel in Form von Betrug, Computerbetrug oder Fälschung beweiserheblicher Daten. Es gibt im deutschen Strafrecht also verschiedene Straftatsbestände, die Datenklau erfassen, aber Identitätsdiebstahl selbst ist keine eigene Straftat, da man Daten nicht stehlen kann. Man kann nur körperliche Sachen, also Dinge, die man anfassen kann, stehlen.

> Immer mehr Menschen verlieren die Fähigkeit, **RICHTIG** zu recherchieren.

Quelle: HSS, Monika Zeitler

Wir brauchen andere Gesetze für den IT-Bereich, meint der Rechtsanwalt und Datenschutzexperte Marc Maisch (l.)

Offensichtlich benötigen wir andere Gesetze …

Auf jeden Fall, ja. Beim größten Identitätsdiebstahl, den ich bearbeite – der Mandant ließ sich von einer WhatsApp-Kommunikation täuschen –, geht es um eine halbe Million Euro, die in Bitcoin abgebucht wurde. Selbst in diesem Fall ist die Polizei nicht in der Lage zu ermitteln. Denn um Bitcoin-Transaktionen nachvollziehen zu können, benötigt man eine spezielle Software, die ungefähr 50.000 Euro im Jahr kostet. Das kann sich nicht jede Polizeidienststelle leisten. Der Erfolg der Ermittlung hängt zudem davon ab, ob das Landeskriminalamt die entsprechenden personellen Kapazitäten hat, denn es muss sich ein Ermittler vor den Computer setzen und jede einzelne Transaktion nach- und zurückverfolgen – das geht nur händisch. Jetzt können Sie sich ausmalen, wie aufwendig so eine Ermittlung ist.

Dann ist der Schutz vor Datenklau umso wichtiger. Wie schützen Sie sich denn davor?

Ein Punkt ist Datensparsamkeit. Ich nutze privat keine sozialen Medien, nur geschäftlich LinkedIn und Xing. Von mir existieren keine privaten Daten, es gibt kein privates Bild im Internet, außer, mich fotografiert jemand auf einer Party und ich konnte mich nicht schnell genug ducken. Niemand kennt mein Geburtsdatum. Ich bin sehr vorsichtig. In einem Hotel im Ausland muss man eine Reisepasskopie abgeben, dabei ist mir immer unwohl. Es ist ein Riesenproblem, dass sämtliche Daten von Prominenten beispielsweise bei Wikipedia stehen …

Über das alles macht man sich zu wenig Gedanken.

Es gibt öffentliche Datenbanken wie „Have I Been Pwned", wo Sie anhand Ihrer E-Mail-Adresse überprüfen können, ob Sie schon Opfer geworden sind oder möglicherweise Opfer werden können, wie viele Data Breach (Datendiebstahl) Sie mit Ihrer Adresse haben. Es geht hier um Datensätze, in denen man E-Mail-Adressen mit Passwörtern und anderen Daten finden kann. Haben Sie dort eine grüne Ampel, ist alles gut. Wenn Sie eine rote Ampel bekommen, schauen Sie mal, ob Sie eine Dropbox haben. Sie wurde 2012 gehackt und dabei sind viele Daten abgeflossen. Mit älteren E-Mail-Adressen hat man bestimmt einen Treffer. Probieren Sie die wohl uralte Adresse Mueller@web.de. Diese nutze ich jetzt immer bei Vorträgen, weil sie 42 Datenschutzvorfälle hat. Da sieht man, was Herr Müller schon alles genutzt hat, vor allem Computerspiele und seine Kombinationen aus E-Mail-Adresse, Passwörtern ...

Das ist grauenhaft, was Sie so alles berichten.

Marc Maisch: Manchmal führe ich Gespräche mit Personen, die von Tätern so bedroht werden, dass sie im Verborgenen bleiben müssen. Handys müssen bei diesen Gesprächen ausgeschaltet sein, weil Instagram immer mithört. Das können Sie nur ändern, wenn Sie in der App das Mikrophon aktiv deaktiviert haben. Instagram gehört zu Facebook und Facebook ist gleich WhatsApp. Das heißt, dass alles dort zusammenläuft. Ich teste das gerne mit Freunden, rede mit ihnen über Snowboard und Skifahren. Auf ihren Geräten blitzt dann plötzlich Snowboard-Werbung auf. Das ist schon krass.

Cem Karakaya: Früher haben wir in der Telefonzelle telefoniert mit geschlossener Tür, damit derjenige, der draußen wartete, nichts von unserem Gespräch mitbekam. Heute haben wir keine Geheimnisse mehr.

Da hat sich viel verändert. Aber lassen Sie uns auf den Punkt bringen, wie ich mich schützen kann.

Marc Maisch: Ein sicheres Passwort mit zwanzig Stellen. Dieses Passwort sollte nur einmal für einen Account verwendet werden, niemals ein Passwort zweimal verwenden. Darüber hinaus ist eine Zwei-Faktor-Authentifizierung von großem Nutzen. Au-

> Ein Opfer von Identitätsdiebstahl muss schnellstens reagieren und sofort **STRAFANZEIGE** erstatten.

ßerdem sollte man mit Daten sehr sparsam umgehen: kein Geburtsdatum im Internet, außer es lässt sich gar nicht vermeiden. Ein privater Tipp von mir: Wenn man nichts bezahlen muss, kann man seinen Geburtstag um drei Tage verschieben, den Monat ändern etc. Laden Sie außerdem aktuelle Updates immer sofort herunter. Diese Sicherheitslücken werden ansonsten ausgenutzt.

Behalten Sie einen gesunden Menschenverstand und lassen Sie sich von Ihrem Bauchgefühl leiten. Wenn ich zum Beispiel ein aktuelles IPhone 13 im Internet sehe, das statt 1.400 Euro nur 300 Euro kostet, dann könnte das Betrug sein. Gehen Sie auch niemals in Vorkasse, sonst ist das Geld weg, wenn es Betrug war. Und Vorsicht ist geboten bei Video-Ident-Verfahren, also nie seinen Personalausweis in die Kamera halten.

Informationen gibt es bei der Verbraucherzentrale oder beim Bundesamt für Sicherheit in der Informationstechnik (BSI). Auch heise.de (https://www.heise.de) ist eine gute Seite, um sich über aktuelle Angriffe zu informieren. Die Volkshochschulen übrigens bieten auch entsprechende Kurse an – und natürlich die Hanns-Seidel-Stiftung.

Vielen Dank an Sie beide für dieses aufschlussreiche Gespräch und für Ihre Tipps und Ratschläge.

Das Gespräch führte Susanne Hornberger, Leiterin Kommunikation und Öffentlichkeitsarbeit der Hanns-Seidel-Stiftung, München. ///

Im Video: Sicherheitstipps gegen Cyberkriminalität von Cem Karakaya

Weitere Informationen und Hilfe

www.bsi.bund.de/DE/Themen/Verbraucherinnen-und Verbraucher/verbraucherinnen-und-verbraucher_node.html
(Bundesamt für Sicherheit in der Informationstechnik)

www.blm.de/files/pdf1/blm-selbstschutz.pdf
(Selbstdatenschutz)

www.klicksafe.de
(Medienkompetenz für Kinder, Eltern und Lehrkräfte)

www.verbraucherzentrale.de/wissen/digitale-welt
(Rechte im Internet)

www.polizei-beratung.de/startseite-und-aktionen/
(polizeiliche Tipps)

www.schau-hin.info
(Elternratgeber)