

SICHERHEITSPRAGE



Von Katja Grieger

Wenn Trennungen gefährlich werden

Mitten unter uns, von vielen aber völlig unbemerkt, gibt es ein riesiges Sicherheitsproblem in diesem Land: häusliche Gewalt gegen Frauen. Jeden dritten Tag wird eine Frau von ihrem Partner oder Ex-Partner getötet, ungefähr genauso viele überleben eine versuchte Tötung. Jedes Jahr zeigen mehr als 100 000 Frauen ihre Männer bei der Polizei an. Das ist aber nur ein Bruchteil der tatsächlich Betroffenen. Jede vierte Frau erlebt mindestens einmal in ihrem Leben Gewalt von ihrem Partner oder ehemaligen Partner.

Warum sprechen so viele Frauen mit niemandem über die Verletzungen, Vergewaltigungen, Drohungen und Demütigungen, die sie zu Hause erleben? Leider kann sich eine Frau nicht sicher sein, dass ihre Umgebung hilfreich reagiert. Wenn Betroffene sich aber jemandem anvertrauen, dann ist die Reaktion dieser Vertrauensperson ganz entscheidend. Relativiert sie die Gewalt und gibt der Betroffenen eine Mitschuld? Oder empört sie sich und bietet Unterstützung an? Die Reaktionen der ersten Ansprechpersonen stellen häufig die Weichen dafür, wie es weitergeht. Deshalb können sich auch Bezugspersonen an eine Beratungsstelle wenden und dort besprechen, wie sie helfen können.



Jedes Jahr zeigen mehr als 100 000 Frauen ihre Männer an.

Ein verbreiteter Irrtum ist, dass in jedem Fall automatisch alles gut wird, sobald sich die Frau vom Partner trennt. Trennungssituationen können für die Betroffenen gefährlich werden, die Gewalt kann sogar noch zunehmen, weil der Mann „seine“ Frau nicht gehen lassen möchte. Gerade wenn es gemeinsame Kinder gibt, hat die Frau oft nicht die Chance, sich in Sicherheit zu bringen, weil trotz der Gewalt ein Umgangsrecht besteht. An dieser Stelle sind Politik und Gerichte gefragt, die Sicherheit von Frauen und Kindern endlich höher zu bewerten als das Umgangsrecht.

Es bleibt viel zu tun, bis auch das eigene Zuhause für Frauen ein sicherer Ort ist. Wir alle können dazu beitragen, indem wir auf das Problem aufmerksam machen, uns mit Betroffenen solidarisieren und hinschauen.

Info Katja Grieger ist Geschäftsführerin des Bundesverbandes Frauenberatungsstellen und Frauennotrufe (BFF).

SMARTE GADGETS

Leuchtende Beispiele für sicheres Fahrradfahren

Smarte Fahrradbeleuchtung bietet allerlei Funktionen, die man ansonsten nur von motorisierten Verkehrsteilnehmern kennt. So können smarte Leuchten etwa einen Richtungswechsel anzeigen und als Blinker beim Abbiegen fungieren. Das geschieht entweder automatisch, über eine am Lenker angebrachte Fernbedienung oder durch Antippen. Durch Aufleuchten signalisieren sie zusätzlich, dass der Fahrer gerade abbremst. Die smarten Gadgets lassen sich entweder rückwärtig am Gepäckträger oder seitwärts an den Haltegriffen befestigen. Wer keine zusätzlichen Gegenstände mit sich herumschleppen möchte, kann sich auch mit blinkenden Handschuhen oder aufleuchtenden Gürteln behelfen. Andere smarte Fahrrad-Gadgets markieren rückwärtig via Laser einen fest abgegrenzten Sicherheitsbereich auf dem Boden, um sonstige Verkehrsteilnehmer auf Abstand zu halten. Smarte Helmkameras regulieren selbstständig und in Abhängigkeit von der Umgebung die Stärke des Lichts und die Ausrichtung des Lichtkegels. Wer sich dann immer noch unsicher fühlt, kann sein Fahrrad mit LED-Beleuchtung bis hin zur rollenden Kirmesbude aufrüsten.



FOTO: MAGNIFIC MICROLIGHTS

heitsbereich auf dem Boden, um sonstige Verkehrsteilnehmer auf Abstand zu halten. Smarte Helmkameras regulieren selbstständig und in Abhängigkeit von der Umgebung die Stärke des Lichts und die Ausrichtung des Lichtkegels. Wer sich dann immer noch unsicher fühlt, kann sein Fahrrad mit LED-Beleuchtung bis hin zur rollenden Kirmesbude aufrüsten.

ZAHLEN, BITTE



11

Prozent der Deutschen bewahren ihr Bargeld im Tresor auf. 3 Prozent verstecken Bargeld im Kleiderschrank oder Bücherregal, ein Prozent der Deutschen hat Geld in der Sockenschublade.

QUELLE: YOUNGOV

Transaktionen mit Tücken



Onlinebanking ist bequem – leider auch für Kriminelle, die Daten ausspähen und dann Konten plündern. Die Bank kommt nur für den Schaden auf, wenn der Kunde selbst nicht unvorsichtig war



Von Marco Tripmaker

Den Herbst vergangenen Jahres wird Bülent K. aus Berlin sicher nicht so schnell vergessen, und das hat nichts mit seinem bestandenen Staatsexamen für das Lehramt zu tun. Nach einem Clubbesuch mit Kollegen und einem Abend mit zwei, drei Bier zu viel stellt der junge Mann fest, dass sein Smartphone verschwunden ist. Und nicht nur das: In der darauf folgenden Woche erfolgt eine Abbuchung von knapp 5000 Euro von seinem Bankkonto auf ein albanisches Konto. Die bislang unbekanntes Täter sichern sich das Geld sofort in bar, sie sind über alle Berge und werden vermutlich niemals gefunden werden. Doch Bülent K. hatte Glück im Unglück: Seine Bank, ein großes und renommiertes Kreditinstitut, erstattete ihm den Betrag. Bülent K. konnte nachweisen, dass er in der Herbstnacht nicht grob fahrlässig gehandelt hat. Banken sind gegen solche Betrügereien versichert. Wie lassen sich Schäden beim Onlinebanking dennoch von vornherein vermeiden?

Cybercrime-Straftaten machen Deutsche skeptisch

Fast 40 Prozent aller Deutschen fühlen sich laut IT-Verband Bitkom unsicher dabei, wenn sie ihren Bankgeschäften im Internet nachgehen. Zu groß sind die heutigen Möglichkeiten im Bereich Cybercrime, „bei denen sich Täter ganz bewusst unerkannt im Untergrund verabreden, um diverse Straftaten zu verüben.

40

Prozent der Deutschen haben kein sicheres Gefühl beim Onlinebanking.

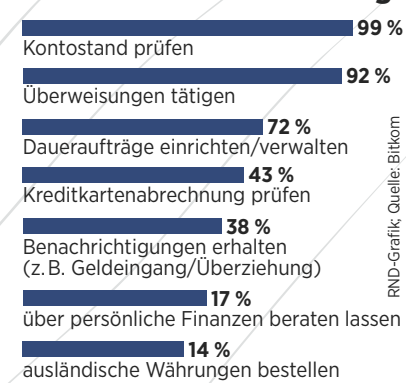
Dabei gibt es top ausgebildete Experten für quasi alle Bereiche. Sie steuern ihre kriminellen Handlungen als Dienstleistung von jedem denkbaren Ort der Welt aus. Wir nennen das „crime as a service“, sagt der Osnabrücker Strafrechtler Arndt Sinn. Ein Täter späht dabei potenzielle Onlinebanking-Opfer aus, der andere löst die technischen Herausforderungen, ein dritter Täter kümmert sich um Buchhaltung und Geldflüsse. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) stuft die Gefährdungslage in seinem aktuellen Lagebericht als weiterhin hoch ein. Die Situation habe sich sogar verschärft und sei im Vergleich zu 2017 vielschichtiger geworden: „Es gibt nach wie vor eine hohe Dynamik der Angreifer bei der Weiterentwick-

lung von Schadprogrammen und Angriffswegen“, heißt es im Bericht.

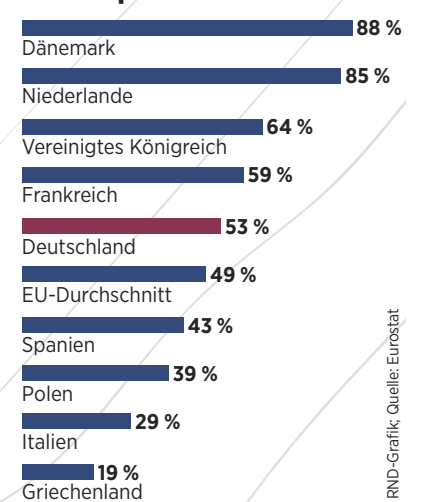
Schadsoftware kommt meistens per E-Mail

„Auch wenn es natürlich ein riesiger Vorteil ist, von jedem Ort der Welt aus mobil seine Bankgeschäfte abzuwickeln – man sollte sich nicht zu naiv im Internet und beim Onlinebanking bewegen, weder am PC noch auf dem Smartphone. Ein vernünftiger Browser wie Apples Safari oder der Windows 10 Edge, eine Firewall oder eine Virtual-Private-Network-Verbindung (VPN) sollte man sich schon zulegen, um gut geschützt zu sein“, sagt Jörn Weber, Geschäftsführer der Corma GmbH, eines Unternehmens für nationale und internationale Wirtschaftsermittlungen.

Genutzte Angebote im Rahmen des Onlinebanking



Onlinebanking-Nutzung in Europa



Geldautomaten werden rar

Bargeldloses Bezahlen verdrängt Bankomaten – komplett verschwinden sollen sie aber nicht

Es gibt nichts mehr zu holen: Immer öfter werden in Deutschland Geldautomaten abgebaut. Die Zahl sinkt stetig. Nach Angaben der Deutschen Kreditwirtschaft (DK), der Interessenvertretung der fünf deutschen kreditwirtschaftlichen Spitzenverbände, zu denen auch der Sparkassen- und Giroverband sowie der Bundesverband der Volks- und Raiffeisenbanken zählen, gab es 2016 noch 60 000 Automaten in der Bundesrepublik; Ende 2017 waren es dagegen nur noch 58 000. Zu teuer und zu unsicher sind die Automaten manchem Geldinstitut.

„Beim Betrieb eines Automaten sind Kosten, Erreichbarkeit und Nutzerverhalten der Kunden zu berücksichtigen. Diese Aspekte sind von Standort zu Standort individuell“, sagt ein DK-Sprecher. Manchem Geldinstitut ist das Betreiben eines Automaten mit Aufwendungen bis zu 25 000 Euro jährlich zu kostenintensiv. Zumal Anschläge auf Automaten die Versicherungskosten tendenziell in die Höhe treiben. Außerdem hat bargeldloses Einkaufen nicht zuletzt durch den Onlinehandel zugenommen. Der Bedarf, Bargeld abzuheben, geht allgemein zurück. Gerade an SB-Standorten seien mehrere Automaten auf einem Fleck häufig überflüssig, heißt es bei der DK. Dennoch sei die flächendeckende Bargeldversorgung nicht in Gefahr. Komplet verschwinden würden die Automaten auch künftig nicht.

Zudem gibt es Alternativen zum Automatengeld. So bieten auch Supermärkte, Drogerien und Tankstellen ihren Kunden an, kostenlos

Geld an der Kasse abzuheben. Bei diesem sogenannten Cashback-Service nennt der Kunde dem Kassierer die Summe, die er ausbezahlt haben möchte. Die Gebühren, die für die Transaktion anfallen, übernehmen die Märkte in der Regel selbst. Da bei Kreditkarten meist höhere Gebühren anfallen, ist das Abheben oft nur mit EC-Karte möglich.

Die meisten Geschäfte legen einen Mindesteinkaufswert fest, der mit der Abbuchungssumme verrechnet wird. Ein Sicherheitsrisiko sieht die DK im Abheben an der Kasse nicht: Für Auszahlungen im Einzelhandel würden die gleichen hohen Sicherheitsstandards wie bei anderen Transaktionen gelten. Zudem sei der Einzelhandel mit dem Handling von Bargeld vertraut, heißt es.



Geld gibt es nicht mehr an jeder Ecke.

FOTO: TOBIAS KLEIN-SCHMIDT/DPA



Zudem sei es dringend angeraten, alle Systeme stets auf dem neuesten Stand zu halten. „90 Prozent der Phishing-Schadsoftware zum Ausspionieren der Transaktionsnummern (TAN) gelangen über E-Mail auf unsere Systeme. In diesem Bereich gilt es, ganz besonders aufmerksam zu sein, damit Täter nicht PC oder Handy kapern können. Auch der TAN-Block in der Schublade ist im Falle eines Einbruchs nicht gerade ideal“, sagt Weber. Eine besonders beliebte Masche: Kriminelle lassen sich, inspiriert von Telefonrechnungen von Mobilfunkgesellschaften, Zweitkarten für Smartphones zuschicken, haben dann Zugriff auf mobile TAN und können in kürzester Zeit komplette Konten plündern. Mittlerweile reagieren Telefongesellschaften offenbar sensibler, wenn es um derartige Anforderungen geht.

„Natürlich ist die Sicherheit auch immer abhängig vom Nutzer.“

Nicole Gemperlein, Onlinebanking-Expertin bei der Hamburger Volksbank

le, schließlich seien mehr als 70 Prozent der Privatgirokonten für Onlinebanking freigeschaltet. „Die Kundenbedürfnisse haben sich geändert. Selbstverständlich bieten wir Online- und Mobilebanking über den PC oder das Smartphone an. Dabei werden die neuesten Sicherheitsstandards immer über unseren genossenschaftlichen Finanzverbund sichergestellt. Für das Handy stellen wir unseren Kunden die VR-Banking-App zur Verfügung“, erläutert Gemperlein. Diese App sei vor allem bei der jungen Klientel ab 16 Jahren sehr beliebt. „Natürlich ist die Sicherheit auch immer abhängig vom Nutzer. Wichtig ist zum Beispiel, dass der Kunde regelmäßig seine Endgeräte aktualisiert und sorgsam mit seinen persönlichen Daten umgeht“, betont Gemperlein. Auf der eigenen Homepage habe das Unternehmen Erklärfilme und nützliche Tipps für die Kunden bereitgestellt.

TAN-Blöcke habe man aus Sicherheitsgründen bereits vor Jahren abgeschafft. Die TAN-App sowie das Smart-TAN-Verfahren mit einem Lesegerät böten einen deutlich höheren Sicherheitsstandard. Dennoch empfiehlt Gemperlein Kunden, die Umsätze auf dem Girokonto regelmäßig zu checken und ungewöhnliche Buchungen sofort der Bank zu melden. „Bei Unregelmäßigkeiten sollte das Onlinebanking umgehend über die einheitliche Hotline 116 116 gesperrt werden.“ Sollte es doch mal unverschuldet zu einem Betrugsfall kommen, greife die Versicherung der Bank, sagt Gemperlein und unterstreicht, dass ein Kreditinstitut nie per E-Mail oder am Telefon Passwörter und Zugangsdaten abfrage.

Wer trotz Vorsichtsmaßnahmen Betrugsoffer wird, sollte nach der Sperrung von EC- oder Kreditkarte auch Anzeige bei der Polizei erstatten.

Tipps des Bundesamts für Sicherheit in der Informationstechnik (BSI)

■ **E-Mail-Phishing - Passwortdiebstahl mit manipulierten E-Mails:** Beim Onlinebanking bestätigt der Kunde mit Passwort, PIN und TAN seine Identität. Kriminelle versuchen, genau diese Daten auszuspähen. Der Fachbegriff hierfür ist Phishing.

■ **Schadsoftware - trojanische Pferde sammeln unbemerkte Daten:** Ein

gesundes Misstrauen schadet nicht, wenn es um Onlinebanking geht. Beim sogenannten Man-in-the-Middle-Angriff überwachen Schadprogramme den Verkehr zwischen Anwender und Bank. Führt der Benutzer eine Überweisung durch, werden Konto sowie Betrag verändert und das Geld ist futsch. Der Anwender bemerkt davon zunächst nichts. Beim

Man-in-the-Browser-Angriff wird hingegen nur die Darstellung der Bank-Website manipuliert.

■ **Mobilebanking - unterwegs lauern Gefahren:** Es ist riskant, fremde Rechner fürs Onlinebanking zu nutzen. Denn Browser speichern Daten der letzten Verbindungen in einem Zwischenspeicher ab - dem sogenannten Cache. Wer Bankge-

schäfte etwa im Internetcafé abwickelt, riskiert, dass Kriminelle später diese Informationen im Cache auslesen. Die Gefahren beim Onlinebanking beschränken sich nicht nur auf PCs. Inzwischen nehmen die Angreifer auch Smartphones und Tabletcomputer ins Visier - auch weil viele Nutzer den Schutzbedarf mobiler Endgeräte noch unterschätzen.

IM TEST

Was tun, wenn's brennt?

Wasserlöscher, Löschspray oder Decke - nicht alles taugt für geschlossene Räume

Es ist ein Horrorszenario, das alle Jahre wieder in der Vorweihnachtszeit in den Schlagzeilen auftaucht. Irgendwo hat ein Adventskranz Feuer gefangen, und in der Folge ist dann ein ganzes Haus abgebrannt. Schlimmer noch als die Sachschäden sind die menschlichen Schicksalsschläge, die mit solchen Unglücken einhergehen.

Wie schnell die Flammen etwa vom Adventskranz auf Möbel und Textilien übergreifen, hat sich auch am Prüfstand der Stiftung Warentest gezeigt. Doch welche Arten von Löschgeräten eignen sich, um kleine Wohnungsbrände im Keim zu ersticken? Die Prüfer haben elf Produkte aus den Bereichen Schaumlöcher, Wasserlöcher, Löschspray, Pulverlöcher und Löschdecke auf ihre Tauglichkeit geprüft. Dafür wurden Adventskranze, Speiseöl und Kabeltrommeln in Brand gesetzt.

So viel vorab: Als besonders praktisch erwiesen sich die Löschsprays mit 0,6 Litern Inhalt von Abus und Prymos. Mit ihnen ließen sich sämtliche Testbrände in etwas mehr als 20 Sekunden löschen. Nur Schaum- und Wasserlöcher mit sechs Litern Inhalt machen das Zuhause noch sicherer, liegen allerdings preislich (55 bis 85 Euro) deutlich über den Löschsprays (knapp 25 Euro). Binnen maximal zwölf Se-

Nicht jedes Löschmittel eignet sich für jede Art von Brand. Daher ist es wichtig, einen Blick auf die Brandklasse zu werfen, die an Löschmitteln ausgewiesen ist: So eignet sich Brandklasse A für Festes - Mobiliar, Textilien oder auch Weihnachtsdekoration. Brandklasse B kommt bei Flüssigem zum Einsatz, etwa bei Spiritus oder Kunststoffen, die sich verflüssigt haben. Für Fett und Öl indes kommen mit einem F gekennzeichnete Löschmittel infrage. Im Test der Stiftung Warentest hat allerdings auch ein mit B gekennzeichnetes Schaumlöcher 0,5 Liter brennendes Speiseöl gelöscht.

kunden waren mit ihnen sämtliche Testbrände gelöscht, die Sprays schafften es immerhin in höchstens 26 Sekunden. Ein wichtiger Tipp der Tester an dieser Stelle: Mit 500 Gramm Löschspray stößt man schnell an Grenzen. Wer ganz auf Nummer sicher gehen will, setzt auf Schaum- und Wasserlöcher mit sechs Litern Inhalt.

Besser die Finger lassen sollte man laut Testern von Pulverlöschern und Löschdecken. Der Haken bei den Löschdecken: Zwar ließ sich das Ausbreiten der Flammen mit ihnen schnell unterdrücken, allerdings ging das Feuer nicht sofort aus, kritisierten die Tester. Ein weiteres Problem: Wer mit Löschdecke löscht, muss gefährlich nah an den Brandherd heran. Vom Löschen brennender Gardinen mit der Decke sahen die Tester daher ab. Ihr Gesamturteil in Sachen Löschdecken: nicht für Laien zu empfehlen! Auch die Pulverlöcher, als günstigere Alternative zu Schaumlöschern beliebt, erfordern etwas mehr Geschicklichkeit: So stufen die Tester sie nur als bedingt einsetztauglich für den Wohnraum ein, denn schon bei einem kurzen Hebeldruck füllt sich ein geschlossener Raum in kürzester Zeit mit einer enormen Pulverwolke. Als Folge ist die Sicht extrem eingeschränkt, das kann gefährliche Folgen haben. Zudem setzt sich das Pulver in Fugen und Ritzen, was zu zusätzlichen Folgekosten führen kann.

Ein naheliegender, aber grundsätzlicher und entscheidender Hinweis der Tester betrifft den Aufbewahrungsort des Löschmittels: Das sollte sich nicht irgendwo in den Untiefen des heimischen Kellers befinden, sondern griffbereit an einer zentralen Stelle aufbewahrt werden - auch wenn es vielleicht einen nicht ganz so hübschen Anblick bietet. Der Gang in den Keller kann im Ernstfall wertvolle Sekunden kosten. Grundsätzlich gilt: Keine Angst vor der Bedienung! Sämtliche Testgeräte waren gut und leicht verständlich beschriftet und konnten schnell zum Einsatz gebracht werden.



Besonders praktisch und effektiv: Löschspray schnitt im Test gut ab.

FOTO: STIFTUNG WARENTEST

Info auf test.de gibt es den kompletten Bericht (kostenpflichtig).

Fakten, Tests, Nützliches

Rund um Ihre Sicherheit:

Hildesheimer Allgemeine Zeitung

www.hildesheimer-allgemeine.de

„Zahlen, wie ich will!“

Kontaktlos bezahlen mit dem Smartphone!

Jeder Mensch hat etwas, das ihn antreibt.

Wir machen den Weg frei.

Mehr Zeit für das, was wirklich wichtig ist. Mit unseren digitalen Karten können Sie per Smartphone und VR-BankingApp bezahlen! Dazu führen Sie die girocard, Mastercard® oder Visa-Karte in digitaler Form im Smartphone mit. Wir erklären Ihnen gerne, wie das geht. www.vb-eg.de

Volksbank eG Hildesheim-Lehrte-Pattensen