Stefanie Bonifer

Cybercrime: Wenn Identität und Existenz in Gefahr geraten

IDENTITÄTSDIEBSTAHL Personenbezogene Daten haben einen hohen Wert. Das spiegelt sich nicht zuletzt in dem kürzlich in Kraft getretenen neuen Datenschutzgesetz wider. Trotz vielfältiger Vorsichtmaßnahmen werden personenbezogene Informationen unbefugt und in großen Mengen gesammelt, im Darknet feilgeboten und dann zu einem wachsenden Teil für kriminelle Handlungen, wie zum Beispiel Betrugsdelikte, verwendet. Jeder kann Opfer sein und läuft damit Risiko, plötzlich die eigene wahre Identität beweisen zu müssen. Dass dies ein schwerer, langwieriger und existenzraubender Prozess ist, zeigt der vorliegende Beitrag eindringlich.

Im November 2018 tagte die Digitalklausur des Bundeskabinetts zum Thema Digitalisierung und künstliche Intelligenz am Hasso-Plattner-Institut in Potsdam. Das Ergebnis ist eindeutig: Deutschland soll digitaler werden – in allen Bereichen. Künstliche Intelligenz (KI) und zunehmende Vernetzung werden uns in vielen, wenn nicht sogar nahezu allen Bereichen des Lebens begegnen. Die Pläne sind ambitioniert: führender Standort im Bereich künstliche Intelligenz, um die Wettbewerbsfähigkeit Deutschlands zu halten, zu sichern und auszubauen. KI soll im Mittelstand und in der Industrie Einzug halten, in Schulen, Universitäten und Ausbildungsinstitutionen und nicht zuletzt auch im Gesundheitswesen.

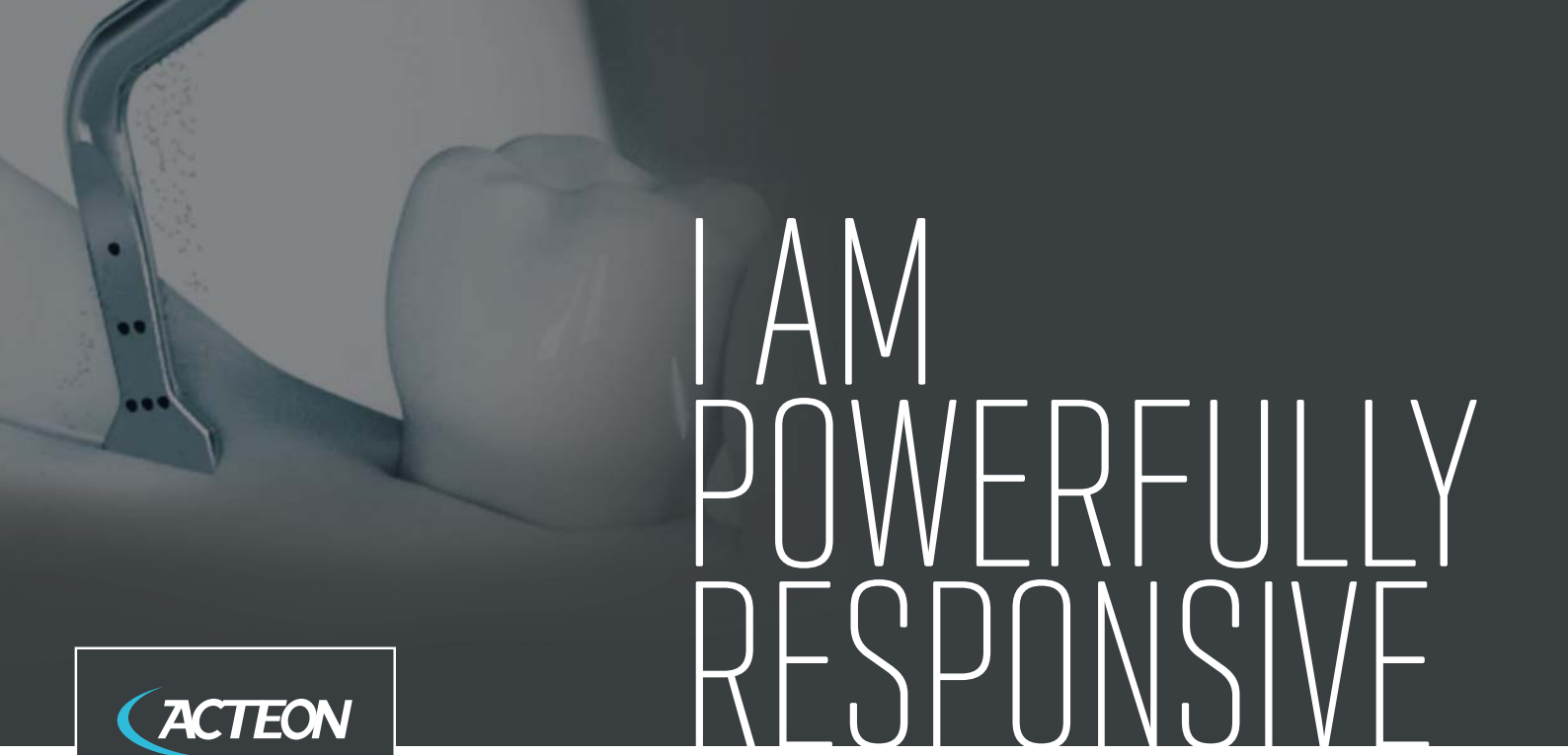
Gefahr durch Übergriffe Unbefugter

Die Vorteile im Gesundheitssektor sind schnell erfasst: KI eröffnet ein großes Potenzial für ein besseres Verständnis von Krankheitsmechanismen und für personalisierte Medizin. Große Mengen an biomedizinischen Daten können dank KI effizienter analysiert und für die Forschung eingesetzt werden. In Zukunft werden wohl vermehrt sogenannte intelligente Geräte in der medizinischen Versorgung bis hin zu Robotern in der häuslichen Pflege zu finden sein. Anonymisierung, Schutz der Privatsphäre und informationelle Selbstbestimmung werden thematisiert. Doch ein Aspekt bleibt fast unberührt – der Schutz persönlicher Daten vor Übergriffen Unbefugter.

Schaden durch Datenklau in Millionenhöhe

Was passiert, wenn persönliche Informationen gestohlen werden? Welche Folgen hat der Diebstahl digitaler Identitäten? Datenklau im Internet und die daraus resultierenden Folgen sind verheerend. Laut einer repräsentativen Bitkom-Studie aus dem Jahr 2017 sind 49 Prozent der deutschen Internetnutzer bereits Opfer von Kriminalität im Internet geworden, 53 Prozent der deutschen Unternehmen sind betroffen. In 2017 waren 89,8 Prozent (62,4 Millionen Menschen) der deutschen Bevölkerung ab 14 Jahren als Internetnutzer erfasst. Das ergibt eine Opferzahl von 30,6 Millionen Menschen. In Deutschland waren in 2017 3,48 Millionen Unternehmen registriert – 1,84 Millionen Unternehmen erlitten durch Cybercrime finanzielle und Reputationsschäden. Der finanzielle Schaden für die deutsche Wirtschaft wird auf 55 Milliarden EUR geschätzt. Der weltweite wirtschaftliche Schaden wird sogar auf 600 Milliarden US-Dollar beziffert. Gemäß der Sicherheitsfirma McAfee sind gut 25 Prozent des Gesamtschadens auf den Diebstahl geistigen Eigentums zurückzuführen.

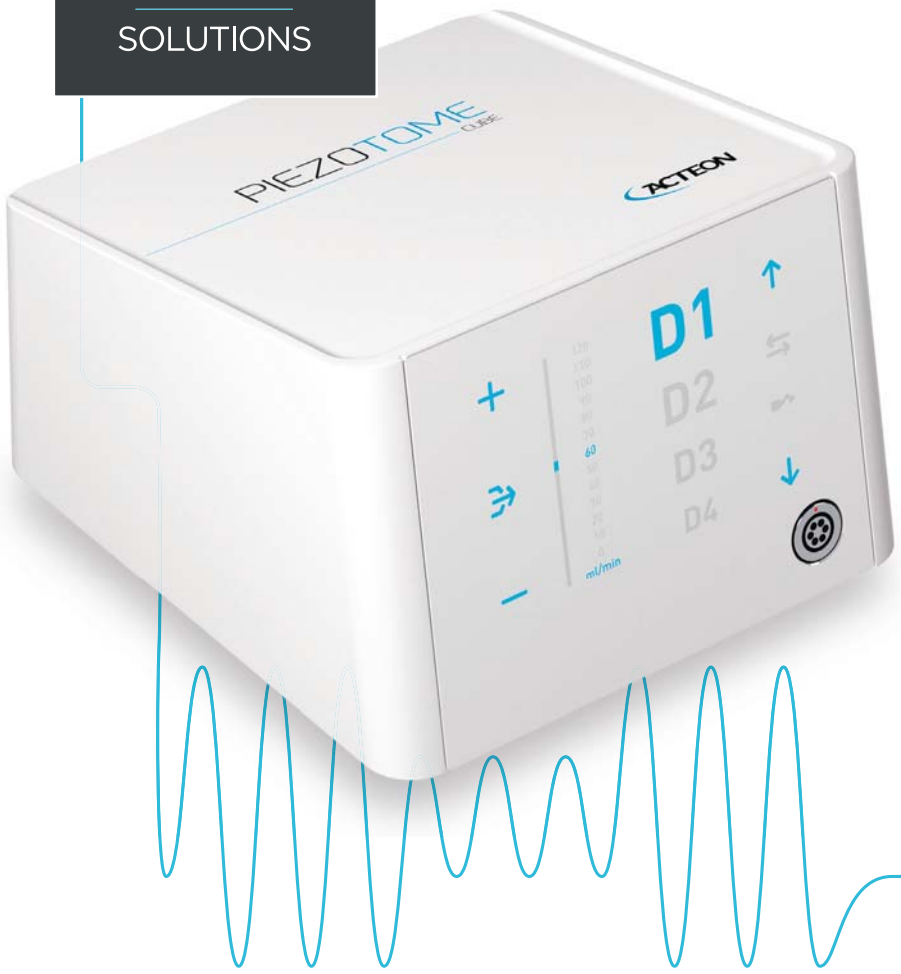
Für die deutsche Wirtschaft basiert der finanzielle Schaden auf Hochrechnungen. Der tatsächliche Schaden fällt



I AM POWERFULLY RESPONSIVE

ACTEON
MINIMALLY
INVASIVE
SOLUTIONS

PIEZOTOME CUBE



für maximalen Knochenerhalt und sofortige Implantation

Extrahieren Sie ohne Stress und Trauma:

- Erhaltung der Integrität des Alveolarknochens
- Schonend für Weichgewebe
- Perfekte Voraussetzung für Sofortimplantation
- Verringerter Kraftaufwand

Bewiesene klinische Vorteile:

- 50 % weniger Schmerz und Schwellung[1]
- 98 % weniger Schmerzmittel notwendig[2]

(1) Cicciù M, Bramanti E, Signorino F, Cicciù A, Sortino F. Experimental study on strength evaluation applied for teeth extraction: An in vivo study. (Experimentelle Studie zum Kraftaufwand für die Zahnextraktion: eine In-Vivo-Studie.) Open Dental J. 2013;7:20-26. Online veröffentlicht am 8. März 2013
(2) Troedhan A, Kurrek A, Wainwright M. Ultrasonic Piezotome surgery: it is a benefit for our patients and does it extend surgery time? A retrospective comparative study on the removal of 100 impacted mandibular 3rd molars. (Chirurgie mit dem Ultraschall-Piezotom – Nützt sie den Patienten und verlängert sie die Dauer des Eingriffs? Eine retrospektive Vergleichsstudie zur Entfernung von 100 mandibulären Weisheitszähnen.) Open Journal of Stomatology. 2011;1:179-184

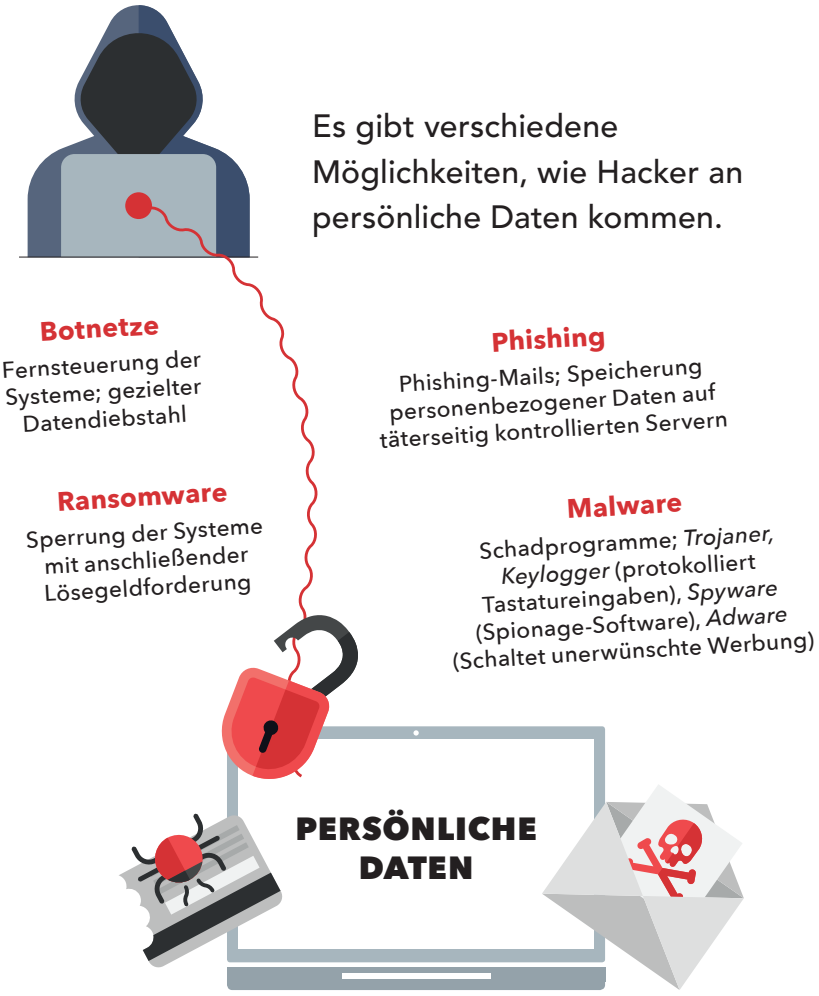
Medizinisches Gerät der Klasse IIa - CE 0459 - Nur für den professionellen Einsatz. Erstelldatum: 05/2018

ACTEON® Germany GmbH | Klaus-Bungert-Strasse 5 | 40468 Düsseldorf
Tel.: +49 (0) 211 / 16 98 00-0 | Fax: +49 211 / 16 98 00-48
info.de@acteongroup.com | www.acteongroup.com

ACTEON

vermutlich höher aus – nur etwa jedes dritte Unternehmen erstattet Anzeige. Die Beweggründe sind unterschiedlich. Oftmals wird aus Angst vor Imageverlusten geschwiegen. Auch werden die Folgen unterschätzt und es daher nicht zur Anzeige gebracht. Doch die Folgen sind weitreichend und in der Regel nicht abschätzbar.

Das große Ziel der Hacker ist eindeutig: personenbezogene Informationen. Dazu zählen Zugangs-, Bank- und Kommunikationsdaten sowie auch persönliche Angaben zu Name, Adresse, Geburtsdatum. Interessant sind alle Daten, die für kriminelle Handlungen genutzt werden können oder gewinnbringend verkauft werden können.



Grafik: Klaus Wilke und OEMUS MEDIA AG/Illustration: kuroksta – stock.adobe.com

Ein nicht zu unterschätzender Aspekt ist die mobile Malware. Mit einer fast 100%igen Abdeckung aller Haushalte in Deutschland mit mobilen Endgeräten (Smartphone, Tablet-PC, Smart-TV etc.) und deren ständige Verbindung zum Internet steigt die Angriffsfläche für mobile Schadprogramme. Häufig sind die Nutzer selbst für die Infizierung mit Trojanern, Spyware etc. verantwortlich. In der Regel können aufgrund engmaschig gestrickter Updatezyklen die Softwarehersteller Sicherheitslücken nicht schließen.

Darknet: Lukrativer Datenmarkt

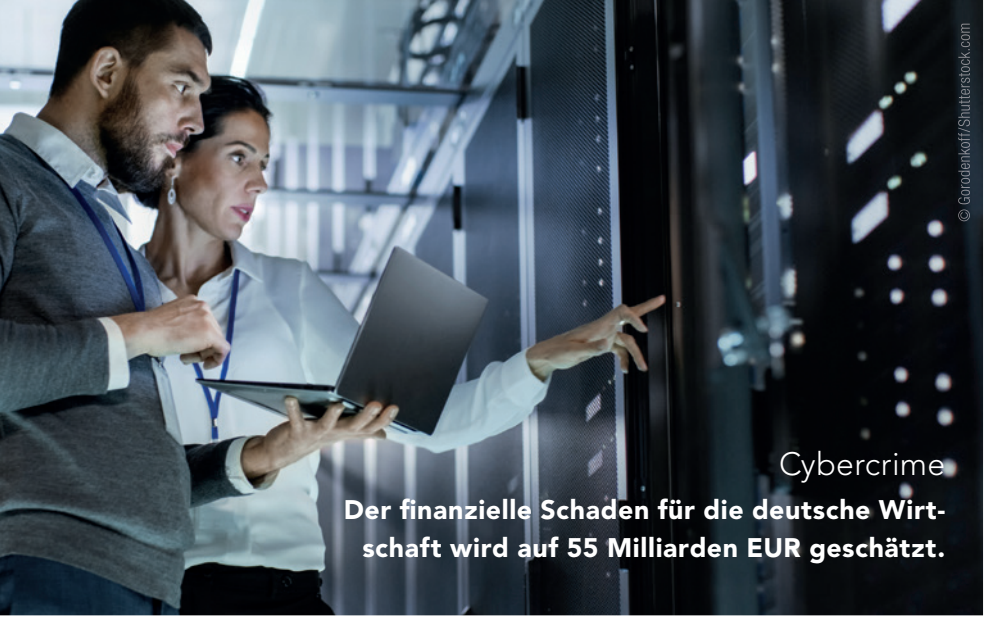
Diese Angaben werden dann in der Regel auf Plattformen im sogenannten Darknet angeboten. Das Bundeskriminalamt stieß in 2017 auf eine geordnete Auflistung von 500 Millionen E-Mail-/Passwortkombinationen, die ein unbekannter Sammler aus vermutlich verschiedenen Quellen über einen bis dahin unbekannten Zeitraum zusammengetragen hat. Die jüngsten Daten stammen aus 2016. Diese Liste wurde kostenfrei zum Download angeboten. Das heißt, es war jedem möglich, die Daten zu beziehen und zu nutzen. Der Webdienst Breach Level Index gibt an, dass bis Ende Juni 2017 rund 1,9 Milliarden Daten gestohlen wurden, 49 Prozent davon in Europa. Die Daten werden oftmals dafür missbraucht, um im Namen der Betroffenen Straftaten zu begehen, oftmals Betrugsdelikte.

Ausnahmezustand Identitätsraub

So erging es auch Klaus Wilke. Seine Daten wurden laut Landeskriminalamt bereits 2013 abgephished und dann 2017 dafür genutzt, um in seinem Namen in einem dubiosen Webshop Werkzeuge anzubieten. Das Geld der Kunden wurde dann ins Ausland überwiesen, die Waren jedoch nicht versendet. So entstand ein Schaden von mehreren 10.000 EUR und eine Anzeige für Herrn Wilke wegen erwerbsmäßigen Betrugs im Internet. Für eine Straftat, die er nicht begangen hat.
Durch die Konfiszierung seines Computers und seines Diensttelefons im Rahmen der laufenden Ermittlungen konnte Herr Wilke seine Kunden nicht weiter betreuen und musste im Zuge dessen seine Selbstständigkeit als Medizinproduktberater aufgeben und gegen eine unzählige Zahl an Hürden ankämpfen. Auf der Suche nach Hilfe und Informationen recherchierte er stundenlang im Internet und fand nur wenig aussagekräftige Anhaltspunkte. Zudem informierte er tagelang sämtliche Vertragspartner darüber, dass seine Daten für betrügerische Zwecke missbraucht wurden: Vermieter, Versicherungen, Energieversorger, Banken, Telefonanbieter etc. Immer wieder schilderte er den Servicemitarbeitern seine Situation, in der Hoffnung auf Hilfe und Entgegenkommen.

Identitätsdiebstahl: Opfer tragen Beweislast!

Oftmals sind die Mitarbeiter aber nicht darüber informiert oder gar befähigt, unterstützende Entscheidungen zu treffen. Die Beweislast liegt in diesen Fällen immer beim Betroffenen. Eine Last, die Betroffene jahrelang begleiten wird – ungerechtfertigte SCHUFA-Einträge, polizeiliche Ermittlungen und ausbleibende Einnahmen. Alle Bemühungen, die folgen, könnten auch einem Hollywood-Thriller entstammen. Die Hauptrolle kann jeder sein – nie-



mand ist vor dem Diebstahl der persönlichen Daten sicher. Dabei ist den Hackern Alter, Geschlecht, Herkunft oder finanzieller Status in der Regel gleichgültig. Wenn man nicht selbst aktiv über einen Leak Checker seine Daten prüft, dann erfährt man auch nur verspätet per Zufall, dass man betroffen ist – bei der Kreditanfrage kommt der negative SCHUFA-Eintrag zur Sprache, bei einer Verkehrskontrolle erfährt man, dass Haftbefehl erlassen wurde … Situationen, auf die vermutlich jeder gerne verzichtet.
Gemäß der aktuellen Gesetzeslage ist der Diebstahl persönlicher Daten noch keine Straftat – erst die kriminelle Handlung, die damit verübt wird, ist gemäß Strafgesetzbuch strafbar. Hier gibt es für die Zukunft noch erheblichen Handlungsbedarf in der deutschen Rechtsprechung.

Projekt bietet erste Anlaufstelle und Hilfe

Das Projekt Safe Cyber Identity wurde von Klaus Wilke ins Leben gerufen, um Opfern von Datenklau und Identitätsdiebstahl im Internet aktive Unterstützung zu geben und gleichzeitig die Möglichkeit zu bieten, in regelmäßigen Abständen in Erfahrung zu bringen, ob die eigenen Daten auf dubiosen Plattformen aufgetaucht sind. Aktuell ist das Projekt noch in der Entwicklungsphase. Zum geplanten Markteintritt im zweiten Quartal 2020 sollen folgende Funktionen umfassende Hilfestellungen bieten:

- sekundenschnelle Prüfung anhand der E-Mail-Adresse, ob persönliche Daten gestohlen wurden
- zyklische Prüfung und regelmäßige Information des Nutzers, ob eigene Daten betroffen sind
- Möglichkeit, die Daten auf nicht eigens initiierten Webseiten/ Webshops zu sperren
- Weiterleitung an kompetente Fachanwälte
- Vorbereiten der polizeilichen Anzeige
- Informationen zum Thema Identitätsdiebstahl und Präventionsmaßnahmen
- bei Betroffenheit wird über einen Automatismus die Wahrscheinlichkeit errechnet, ob die eigenen Daten für kriminelle Machenschaften verwendet werden

Ausblick

Aktuell sind Gespräche mit dem Bundesnachrichtendienst, dem Landeskriminalamt und dem Landesdatenschutzbeauftragten angesetzt, um Schnittstellen und die zukünftige Zusammenarbeit zu eruieren. Mit seinem Projekt Safe Cyber Identity leistet Klaus Wilke einen wichtigen Beitrag, die Sicherheit persönlicher Daten im Internet zu verstärken und die öffentliche Aufmerksamkeit für diese sensible Thematik zu intensivieren.

Info:
Klaus Wilke steht für Vorträge zum Thema „Sicherheit persönlicher Daten im Internet“ zur Verfügung.
Anfragen bitte an: **mvs.wilke@gmail.com**

Eine finanzielle Unterstützung für die Ausführung des Projektes Cyber Safe Identity ist möglich. Mehr Informationen zur Sammelaktion unter www.mvs-wilke.de

INFORMATION

MVS Wilke
Inh. Klaus Wilke
Wacholdersteig 7
14822 Borkheide
Tel.: 0152 31037141
mvs.wilke@gmail.com
www.mvs-wilke.de