

# DSGVO      Neuigkeiten      vom 09.04.2023

Das Landgericht Leipzig macht Quad9 zum Täter von Urheberrechtsverletzungen. Müssen DNS-Betreiber jetzt mit hohen Geld- oder Haftstrafen rechnen?



## Markt + Trends | IT-Recht & Datenschutz

DNS-Server lösen Namen zu IP-Adressen auf und sind essenziell fürs Surfen. Wer nicht die Standard-Server der Provider nutzt, surft schneller und ohne Blockaden.

### **Durchsetzung der DSGVO soll EU-weit harmonisiert werden**

Die EU-Kommission strebt eine verbesserte Rechtsdurchsetzung

der Datenschutz-Grundverordnung an. Hierzu sollen die Verfahrensvorschriften zur DSGVO-Durchsetzung harmonisiert werden. Konkret soll es dabei um eine Verbesserung der Zusammenarbeit zwischen den Datenschutzbehörden der verschiedenen EU-Staaten gehen. Hinzukommen sollen die Festlegung von Verfahrensfristen, die Bereitstellung von Instrumenten und die Anforderungen an den Informationsaustausch. Zu guter Letzt sollen die Position der Beschwerdeführer und der Betroffenen gestärkt werden.

Die geplanten Änderungen gehen unter anderem darauf zurück, dass die irische Datenschutzbehörde in der Kritik der anderen EU-Datenschutzbehörden steht. Der Vorwurf lautet auf einen zu nachgiebigen Umgang mit in Irland ansässigen internationalen Unternehmen, darunter Meta, Alphabet und Facebook. Die Beschwerden über zu niedrige Bußgelder oder eine zu lange Verfahrensdauer mehren sich. *Tobias Haar* ([fo@ix.de](mailto:fo@ix.de))

## **Europäischer Datenschutzausschuss gibt grünes Licht für EU-US Data Privacy Framework**

Mit Spannung wurde die Stellungnahme des Europäischen Datenschutzausschusses (EDSA) zum geplanten EU-US Data Privacy Framework erwartet. Doch sie fiel anders aus als von vielen Beobachtern erwartet: Zwar kritisiert der EDSA Einzelaspekte des Rahmens für die DSGVO-konforme Übermittlung von personenbezogenen Daten in die USA, die erwartete völlige Ablehnung blieb jedoch aus.

Eine formale Verabschiedung des Frameworks dürfte damit nur noch eine Frage der Zeit sein. Die Chancen auf dessen Bestand auch bei sich anschließenden Gerichtsverfahren sind damit ebenfalls gestiegen.

In seiner Stellungnahme betont der EDSA deutliche

Verbesserungen unter anderem im Bereich der Rechtsbehelfe gegen Verstöße der US-amerikanischen Zusagen beim Datenschutz. Zu diesen Zusagen äußert sich beispielsweise der Bundesdatenschutzbeauftragte Ulrich Kelber: „Wir sehen den Willen, ein angemessenes Schutzniveau für Betroffene, deren personenbezogenen Daten an Unternehmen in die USA übermittelt werden, zu schaffen.“

Allerdings kommt es nach Auffassung des hamburgischen Datenschutzbeauftragten Thomas Fuchs darauf an, wie diese Vorgaben sich in der Praxis bewähren. „Ob und inwiefern tatsächlich Geheimdienstaktivitäten auf ein verhältnismäßiges Maß reduziert werden und wirksamer Rechtsschutz gewährleistet ist, kann nur die Umsetzung in der Praxis zeigen“, so Fuchs. Tobias Haar ([fo@ix.de](mailto:fo@ix.de))

## **Fragen des Urheberrechtsschutzes für KI-generierte Bilder**

Unter Einsatz von künstlicher Intelligenz durch einen Computer generierte Bilder genießen keinen Schutz nach den Urheberrechtsgesetzen: Darauf hat das United States Copyright Office hingewiesen. In ihrer Einschätzung folgt die Behörde den urheberrechtlichen Vorschriften, die nur schöpferische Leistungen von Menschen erfassen. Auch hierzulande fallen nur „persönliche geistige Schöpfungen“ unter das Urheberrecht. Ob und wie KI-generierte Inhalte zukünftig geschützt werden sollen, diskutieren Juristen derzeit weltweit.

Andererseits können Bilder von KI-gestützten Generatoren urheberrechtlich geschützte Werke enthalten. Zu diesem Ergebnis kam eine Studie der Alphabet-Töchter Google und DeepMind, der University of California in Berkeley, der ETH Zürich sowie der Princeton University. Mit bestimmten Prompts konnten sie Kopien bestehender Werke als KI-Output erzeugen. Deren Nutzung könnte folglich zu einem Urheberrechtsverstoß führen. Denkbar ist dies auch bei textlichen oder sonstigen

Ergebnissen von KI-Generatoren wie ChatGPT. *Tobias Haar*  
([fo@ix.de](mailto:fo@ix.de))

## Onlinezugangsgesetz 2.0: Kritik an Gesetzesentwurf der Bundesregierung

Die Bundesregierung will die Digitalisierung der Verwaltung beschleunigen und hat einen Entwurf für eine Überarbeitung des Onlinezugangsgesetzes vorgelegt. Ziel ist eine einfache, moderne und digitale Verfahrensabwicklung. Geplant sind etwa die Bereitstellung von zentralen Basisdiensten durch den Bund, wodurch landeseigene Entwicklungen für Bürgerkonto und Postfächer entfallen. Zudem soll der Ersatz der Schriftform durch elektronische Signaturen vorangetrieben werden. Auch auf Nutzerfreundlichkeit und Barrierefreiheit soll geachtet werden.

Der Gesetzesentwurf ist vielfach auf Kritik gestoßen. Der Bundesverband der Deutschen Industrie vermisst die Setzung von Standards und Schnittstellen für die digitale Verwaltung. Er fordert zudem eine „Ende-zu-Ende-Digitalisierungspflicht“, also eine rein digitale Verarbeitung von online gestellten Anträgen in den Behörden. Gefordert werden auch vom Bund zentral bereitgestellte Infrastrukturen wie Cloud-Betriebsplattformen oder Bezahlungsfunktionen. Kritisiert wird zudem, dass keine Umsetzungsfristen, sondern nun nur noch eine begleitende Evaluierung vorgesehen ist. *Tobias Haar* ([fo@ix.de](mailto:fo@ix.de))

### Kurz notiert

Das Gesetz zum **Schutz von Whistleblowern** ist vorerst gescheitert. Der Bundesrat hat das vom Bundestag im Dezember beschlossene Gesetz abgelehnt. Gegen Deutschland läuft ein Verfahren der EU-Kommission wegen der verspäteten Umsetzung der Whistleblower-Richtlinie.

Der Bundesdatenschutzbeauftragte hat der Bundesregierung den

**Betrieb einer Facebook-Fanpage** untersagt. Nach derzeitiger Rechtslage ist die damit verbundene Datenübermittlung an Meta rechtswidrig, so die Begründung.

Ob **Cheat-Software für Computerspiele** gegen das Urheberrecht verstößt, soll nun der Europäische Gerichtshof klären. Der Bundesgerichtshof hat die für die Games-Branche wichtige Frage zur Entscheidung den EU-Kollegen vorgelegt.

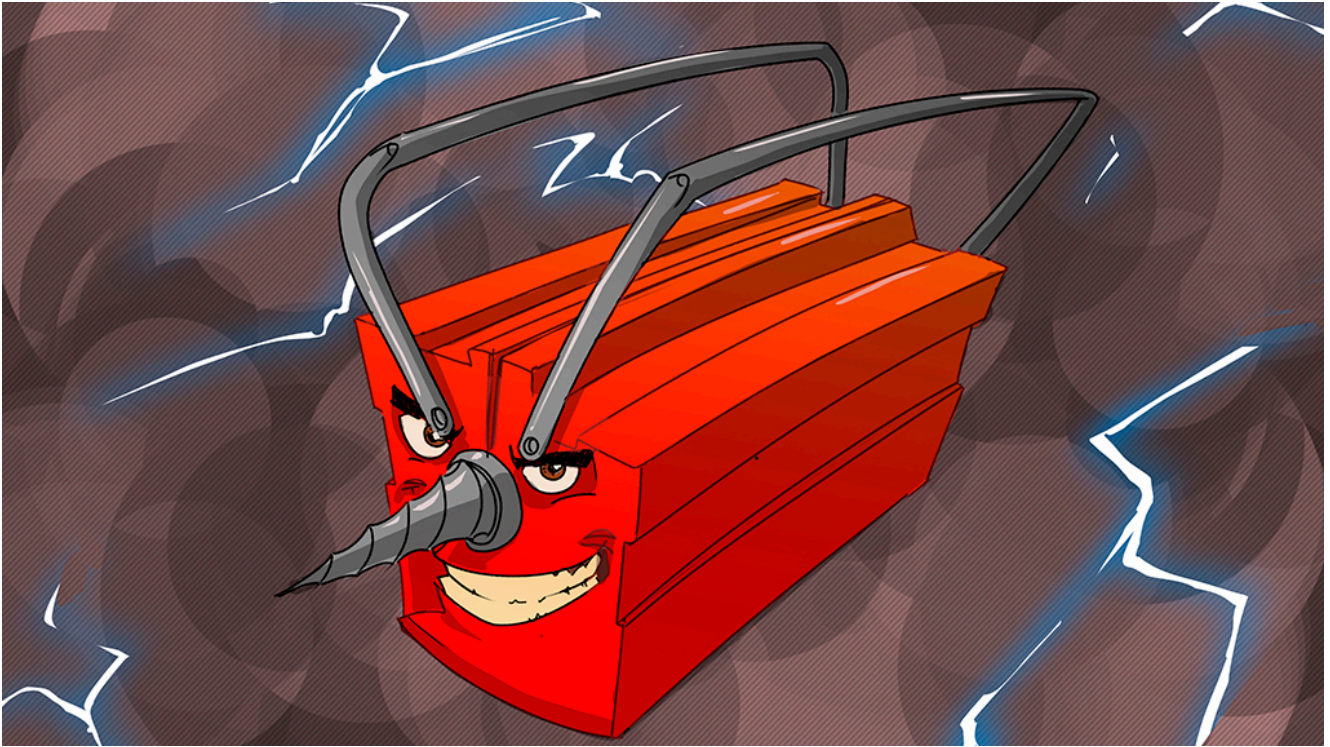
Wer wegen Wettbewerbsverstößen zur Unterlassung bestimmter Inhalte auf Webseiten verpflichtet ist, ist nicht für Altversionen von **Webseiten in der Wayback Machine** verantwortlich. Das hat das Landgericht Karlsruhe entschieden.

Das Landgericht Ravensburg hat die **Entsperrung eines Mobiltelefons** per Fingerabdruck gegen den Willen eines Verdächtigen als rechtmäßig eingestuft.

Der in Kraft getretene **EU Digital Services Act** sieht eine Finanzierung der Aufsicht über sehr große Plattformen über Gebühren vor. Facebook und Co. werden dafür künftig mit bis zu 0,05 Prozent ihres weltweiten Jahresumsatzes zur Kasse gebeten.

---

## **Rechtliche Unsicherheiten bei Hacking-Werkzeug**



## **Kommt drauf an, wozu**

Um Schwachstellen im eigenen Netz zu suchen und Datenflüsse zu überwachen, nutzen Administratoren vielfach die gleichen Softwarehilfsmittel wie Angreifer, die illegale Ziele verfolgen. Was sagt das deutsche Recht dazu? Steht jemand, der mit trickreichen Analyse- und Spähtools arbeitet, mit einem Bei...

## **Kommt drauf an, wozu**

# **Rechtliche Unsicherheiten bei Hacking-Werkzeug**

Um Schwachstellen im eigenen Netz zu suchen und Datenflüsse zu überwachen, nutzen Administratoren vielfach die gleichen Softwarehilfsmittel wie Angreifer, die illegale Ziele verfolgen. Was sagt das deutsche Recht dazu? Steht jemand, der mit trickreichen Analyse- und Spähtools arbeitet, mit einem Bein vor Gericht?

Von Verena Ehrl

Der Theaterautor und Sprachliebhaber Hans-Joachim Haecker brachte die Dual-Use-Problematik bereits 1968 in einem Gedichtchen seines Bandes „Insonderheit“ unter dem Eindruck des internationalen Wettrüstens scherzhaft auf den Punkt:

*„Insonderheit die Abwehrwaffen  
sind für die Abwehr wie geschaffen.  
Auch kann man mit geschickten Händen  
sie für den Angriff gut verwenden.“*

Die Waffen, mit denen Akteure innerhalb der IT-Welt hantieren, eignen sich zum Eindringen in Systeme, zum Überwinden von Sicherungsmaßnahmen, zum Spionieren und Manipulieren. Dieselben Werkzeuge können aber dazu dienen, unterschiedliche Ziele zu erreichen. In der Hand eines Administrators, der ein System, für das er verantwortlich ist, Penetration Tests („Pentests“) aussetzt, kann etwa das Software-Tool „Mimikatz“ legalen Einsatz finden (S. 24). Es ebnet allerdings ebenso gut Angreifern den Weg bei illegalen Aktionen, indem es ihnen Zugangsdaten für die Übernahme eines Netzwerks offenbart. Auf diese Ambivalenz bezieht sich das Schlagwort „Dual Use“ im Zusammenhang mit Hackerausrüstung.

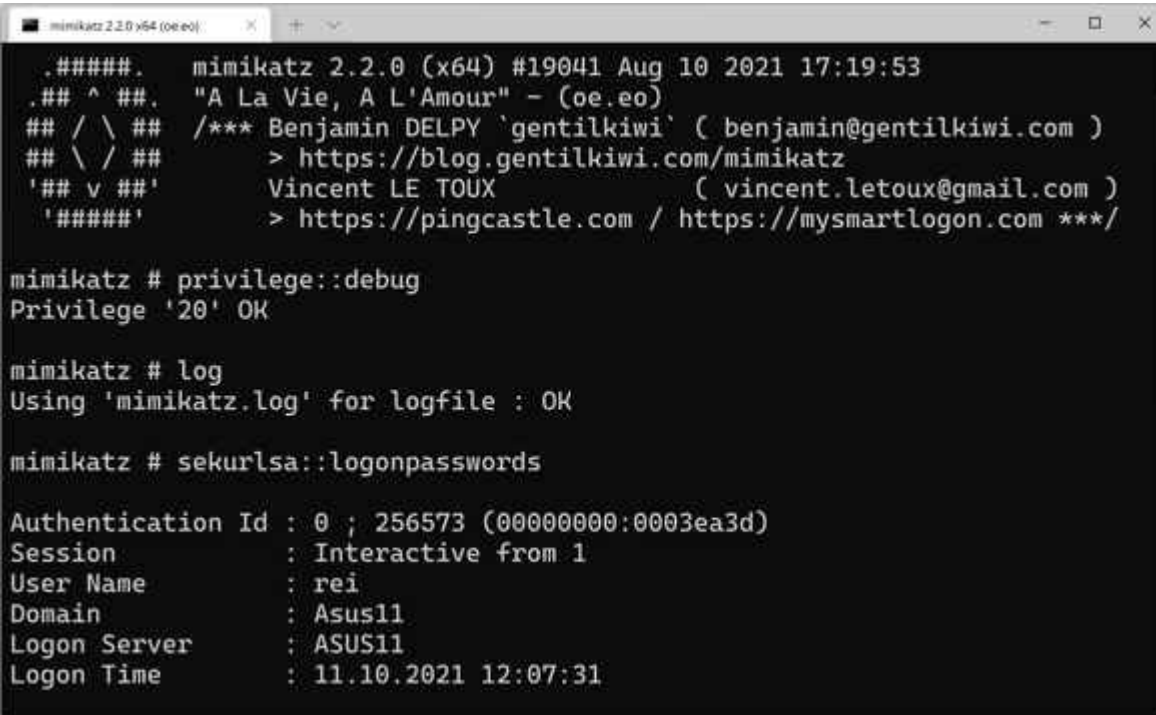
Nicht immer erscheinen die Werkzeuge, um die es geht, so spektakulär wie die Hacking-Gadget-Hardware, mit der c't sich in Ausgabe 18/2017 befasst hat [1]. Sehr oft steht vielmehr bloße Software im Mittelpunkt, die loggt, sucht, entschlüsselt, ausliest, analysiert und speichert (S. 16, 18, 24 und 39). Die rechtlichen Fragen, vor die ein Anwender gestellt ist, sind jedoch grundsätzlich die gleichen wie bei den Spionagegeräten [2]: Wo liegt die rote Linie, jenseits der man sich auf illegalem Terrain bewegt? Was sagt das geltende Recht zum Umgang mit potenziell gefährlichen und schadenträchtigen Tools?

Dass es „Güter mit doppeltem Verwendungszweck“ gibt, die sich

gleichermaßen für legales und illegales Tun eignen, beschäftigt nicht zuletzt den europäischen Gesetzgeber. Am 9. September 2021 ist die Neufassung der sogenannten Dual-Use-Verordnung in Kraft getreten [3].

Sie betrifft „Güter einschließlich Datenverarbeitungsprogramme (Software) und Technologie, die sowohl für zivile als auch für militärische Zwecke verwendet werden können“. Es gibt durchaus Softwareentwicklungsprojekte, die man mit etwas Fantasie in den Betrachtungshorizont der Verordnung rücken kann.

Ziel der Dual-Use-Verordnung ist die Exportkontrolle. Die kann bereits relevant werden, wenn Forschung und Produktentwicklung mit Partnerunternehmen in bestimmten außereuropäischen Ländern stattfinden und dabei schadenträchtige Software im Spiel ist.



```
mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # log
Using 'mimikatz.log' for logfile : OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 256573 (00000000:0003ea3d)
Session           : Interactive from 1
User Name         : rei
Domain           : Asus11
Logon Server      : ASUS11
Logon Time        : 11.10.2021 12:07:31
```

Mimikatz ist ein typisches Beispiel für ein Hackerwerkzeug, das auch verantwortungsvollen Admins wertvolle Dienste leistet, wenn es ums Aufspüren von Schwachstellen im eigenen Netz geht.

Neu im Blick der europäischen Rechtssetzungsorgane und der zur Umsetzung verpflichteten Mitgliedsstaaten sind Länder, welche die Todesstrafe praktizieren oder in denen Menschenrechtsverletzungen wie Folter auf staatliches Geheiß

stattfinden. Wer etwa potenziell gefährliche Software ins nichteuropäische Ausland transferieren will, braucht dazu eine vorherige Genehmigung des Bundesamts für Wirtschaft und Ausfuhrkontrolle (BAFA). Diese Behörde entscheidet in jedem Einzelfall, ob der Transfer zulässig ist oder nicht.

## **Zweierlei Paar Schuhe**

Abseits der von der Verordnung erfassten Transferproblematik sind Dual-Use-Softwarewerkzeuge rechtlich schwer zu fassen. Weder ihr Erwerb noch ihr Besitz ist grundsätzlich untersagt. Straf- und Zivilrecht melden sich erst dann, wenn jemand diese Tools einsetzt, um Rechtsbrüche zu begehen. Derjenige riskiert dann eine Strafe oder er sieht sich zivilrechtlichen Ansprüchen ausgesetzt – oft droht ihm beides.

Nicht alles, was jemand rechtswidrig tut, ist auch strafbar. Mit dem Strafrecht geht der Staat gegen von ihm untersagtes Verhalten vor, dabei sind Strafermittlungsbehörden im Spiel, es gibt Beschuldigung und Anklage. Im Zivilrecht stehen hingegen gleichberechtigte Streitparteien einander gegenüber. Dabei gibt es Kläger und Beklagte, die Gerichte entscheiden über Ansprüche, welche die Parteien gegeneinander geltend machen. Vertragspflichten und Schadenersatzansprüche sind typisches zivilrechtliches Geschäft.

Durch Software kann ein Anwender sich Ärger in beiden Rechtsbereichen einhandeln. Ein gutes Beispiel für die rechtliche Gratwanderung dabei sind die bereits angesprochenen Pentests. Sie haben die Aufgabe, Schwachstellen in Konfiguration, Hard- und Software von Servern, Routern und Arbeitsplätzen im Netz aufzuzeigen. Ein Mitarbeiter, der einen solchen Test im Auftrag eines zuständigen Entscheiders für das betroffene Netz durchführt, bewegt sich damit auf der legalen Seite. Wenn allerdings etwa ein Cybersecurity-Dienstleister einen Pentest unaufgefordert und ohne Erlaubnis bei einem potenziellen Kunden durchführt, um diesen als Auftraggeber zu gewinnen, setzt er sich strafrechtlicher Verfolgung wegen

Datenveränderung oder Computersabotage aus.

Wesentlich sind dabei die Paragraphen 303a und 303b des Strafgesetzbuchs (StGB), die sich mit virtueller Sachbeschädigung befassen. Damit hat der Gesetzgeber 1986 eine Regelungslücke beim Straftatbestand der Sachbeschädigung (§ 303 StGB) geschlossen. Die klassische Sachbeschädigung setzt einen körperlichen Gegenstand voraus – das lässt Daten und beispielsweise Festplatten, die funktionsfähig bleiben, aber deren Inhalt gelöscht oder verschlüsselt wurde, außen vor.

§ 303a StGB stellt die unbefugte Veränderung von Daten unter Strafe. Dort heißt es in Absatz 1: „Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.“

Bereits der Versuch ist strafbar; dasselbe gilt wie beim Ausspähen (§ 202a StGB) und Abfangen von Daten (§ 202b StGB) auch fürs „Vorbereiten“ einer rechtswidrigen Datenveränderung – beispielsweise durch Bereitstellen von Software, deren „Zweck die Begehung einer solchen Tat ist“ (§ 202c Abs. 1 Nr. 2 StGB).

Als Daten in diesem Sinne gelten nach § 202 StGB „nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden“, also nicht etwa Papiernotizen.



verändert wird. Auch hierbei sind wie bei der Datenveränderung bereits Versuch und Vorbereitung strafbar.

Dass es nur ums Stören von Datenverarbeitungen von „wesentlicher Bedeutung“ geht, soll Bagatellfälle aus dem Blick der Strafjustiz nehmen.

## **Erpressungstrojaner vor Gericht**

Im April 2021 hat der Bundesgerichtshof (BGH) einen Fall entschieden, der die Verteilung von Ransomware betraf – also das Einschleusen von Verschlüsselungstrojanern zu Erpressungszwecken [4]. Dabei stufte das Gericht unter anderem das Anbringen einer Eintragung in der Windows-Registry, die das automatische Laden einer Schadsoftware beim Rechnerstart bewirkte, als strafbare Datenveränderung ein. Zugleich sah der BGH in diesem Fall auch eine Computersabotage nach § 303b StGB.

Der Angeklagte war Mitglied einer Cybercrime-Bande mit Sitz in der Ukraine. Diese hatte mit ihren Ransomware-Angriffen von 2013 bis 2016 über 200 Millionen Rechnersysteme infiziert und von den geschädigten Computernutzern mehr als neun Millionen Euro erpressen können.

Schadsoftware ähnlicher Art mit einer vorgesehenen Entsperrmöglichkeit hätte aber auch im Rahmen eines Pentests in einem lokalen Netz durchaus legal verwendet werden können. Ein Unternehmen hätte damit etwa seine Mitarbeiter auf deren Vorsicht testen können, was das Anklicken unbekannter Inhalte betrifft.

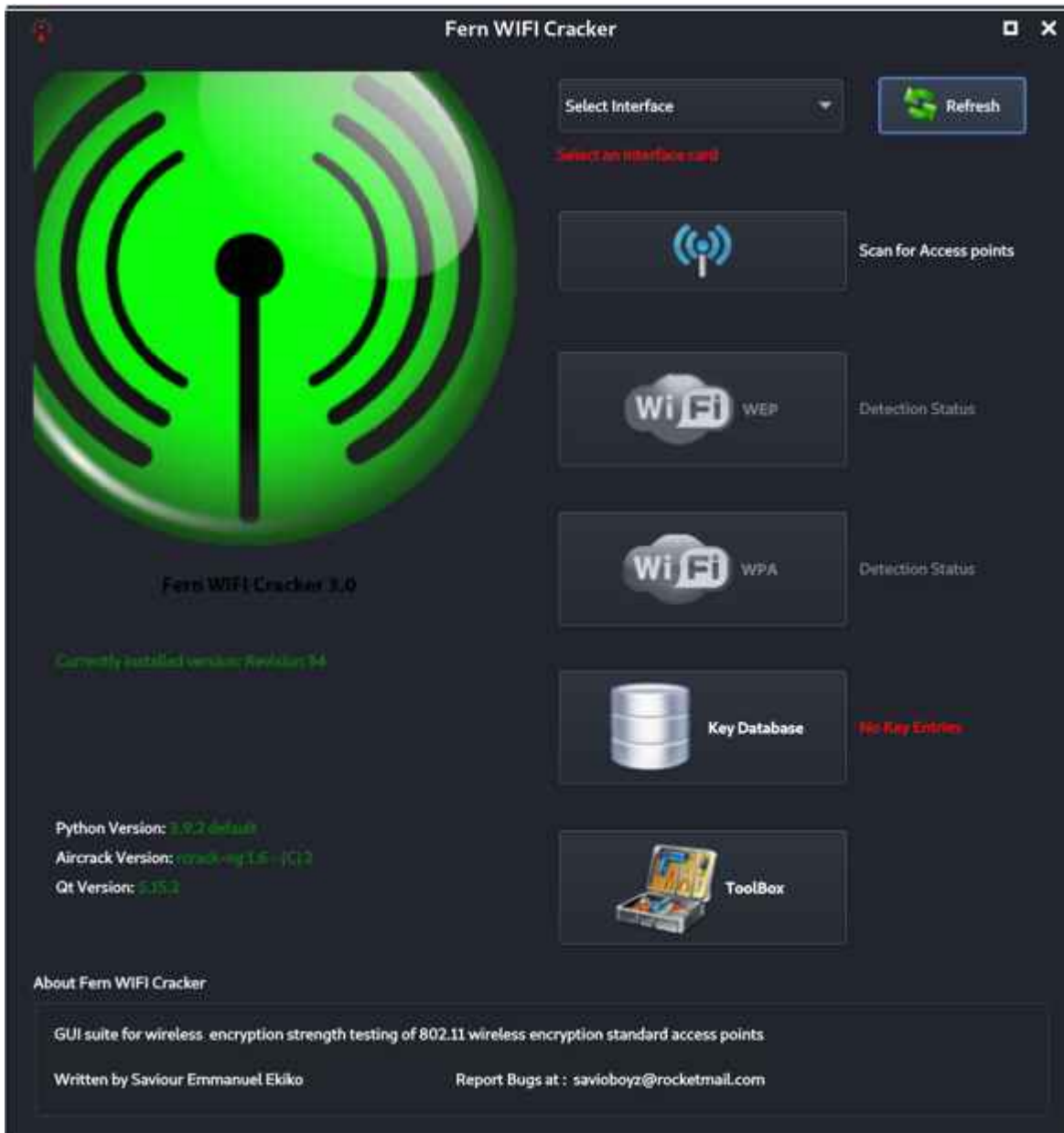
## **Computersabotage am Arbeitsplatz**

Das mutwillige Stören des Datenverarbeitungsbetriebs kann nicht nur strafrechtliche, sondern auch arbeitsrechtliche Auswirkungen haben. Mitarbeiter, die aus Wut oder infolge von Rachegeanken gegen ihren Arbeitgeber Datenvandalismus im

Unternehmensnetz betreiben, riskieren eine fristlose Kündigung.

Das geschah 2019 einem als Key-Account-Manager beschäftigten Arbeitnehmer nach einer heimlichen Löschaktion auf dem Unternehmensserver seines Arbeitgebers. Nach einer Abmahnung war ihm zuvor ein Aufhebungsvertrag angeboten worden. Daraufhin löschte er 8 GByte an Daten, darunter Kalkulationssoftware, Umsatzmeldungen, Vorlagen für Preislisten und Wettbewerbsanalysen für bestimmte Produkte. Die Daten konnten später wiederhergestellt werden. Der Verdacht fiel auf ihn. Gegen die fristlose Kündigung, die er wenig später erhielt, wehrte er sich zunächst erfolgreich. In der Berufungsinstanz jedoch unterlag er vor dem Landesarbeitsgericht (LAG) Baden-Württemberg im September 2020 [5]. Sein Arbeitgeber hatte einen 93seitigen Vergleich des Datenbestands im fraglichen Verzeichnis vor und nach der Löschaktion vorgelegt.

Das Gericht sah die fristlose außerordentliche Kündigung als begründet an: Das unbefugte vorsätzliche Löschen betrieblicher Daten auf EDV-Anlagen des Arbeitgebers taue ebenso wie das Vernichten von Verwaltungsvorgängen grundsätzlich als „wichtiger Grund“ für eine solche Kündigung im Sinne des § 626 Abs. 1 BGB. Dabei komme es nicht unbedingt darauf an, ob sich der Arbeitnehmer nach § 303a StGB oder § 303b StGB strafbar gemacht habe. Es sei auch nicht entscheidend, ob und mit welchem Aufwand ein Teil der gelöschten Daten wiederhergestellt werden konnte oder ob der Arbeitgeber diese Daten für den weiteren Geschäftsablauf tatsächlich benötigte. Vielmehr gehöre es zu den vertraglichen Nebenpflichten eines Arbeitsverhältnisses im Sinne des § 241 Abs. 2 BGB, dass der Arbeitnehmer seinem Arbeitgeber den Zugriff auf betriebliche Dateien nicht verwehre oder unmöglich mache.



In der Hand von Angreifern kann auch der Fern Wifi Cracker, mit dem man Drahtlosnetze auf Sicherheitslücken abklopft, zum Werkzeug für eine Straftat werden.

## Wenn der Admin spioniert

Dass es bei der strafrechtlichen Bewertung von Hacker-Aktivitäten nicht so sehr um die benutzten Werkzeuge als vielmehr um Zweck und Absicht des Einsatzes geht, illustriert auch ein Fall, den 2020 der BGH in letzter Instanz entschied [5]. Zwei Männer mussten sich wegen des Ausspähens von Daten (§ 202a StGB) verantworten. Einer davon leitete die Stabsstelle eines Apothekerverbandes und betrieb daneben ein gesundheitspolitisches Informationsportal im Internet. Der

zweite Angeklagte arbeitete als Systemadministrator am Berliner Standort des Bundesgesundheitsministeriums (BMG) und war nebenbei als Callboy tätig – daher rührte auch die Bekanntschaft der beiden Männer.

Der Admin hatte jahrelang Zugriffsrecht auf alle E-Mail-Accounts seiner Dienststelle und versorgte den Portalbetreiber mit so gewonnenen Interna aus dem Ministerium. Nachdem das Ministerium den unbeschränkten Mailzugriff der Administratoren im Hause als Sicherheitsmangel erkannt hatte, wurde es für den Mann schwieriger – er verlegte sich schließlich auf einen unter den Admins bekannten Notfalltrick, mit dem er sich selbst von Fall zu Fall die nötigen Zugriffsrechte verschaffte. Er lieferte dem Portalbetreiber auf Datenträger kopierte E-Mail-Inhalte nach Wunsch und kassierte dafür insgesamt rund 1000 Euro. Sein Kunde war besonders an E-Mails der Minister und Staatssekretäre sowie einiger Abteilungs- und Referatsleiter interessiert. In den weitergereichten Mails ging es unter anderem um Gesetzesvorhaben, die für das Publikum des Portals besonders interessant waren.

Das Landgericht (LG) Berlin verurteilte die Männer im April 2019 wegen gemeinschaftlichen Ausspähens von Daten nach § 202a StGB und sah in der Manipulation der Zugriffsrechte auf die einzelnen E-Mail-Konten zudem die Überwindung einer Zugangssicherung nach § 202a Abs. 1 StGB. Die gegen das landgerichtliche Urteil eingelegte Revision wies der BGH weitgehend ab, lediglich den einzuziehenden Geldbetrag setzte er niedriger an als die Vorinstanz.

Die Bundesrichter beschäftigten sich vor allem damit, ob Daten im Sinn des §202a Abs. 1 StGB überhaupt als gesichert gelten können, wenn ein Admin mithilfe seiner Kenntnisse darauf zugreifen kann. Die Antwort: Es genüge, wenn getroffene Vorkehrungen den Zugriff auf Daten zumindest deutlich erschweren. Die Sicherung von E-Mail-Accounts durch Passwörter reiche aus. Dabei brauche der Systembetreiber nur den Zugriff Unbefugter zu berücksichtigen, aber nicht die

Zugriffsmöglichkeit durch Eingeweihte oder Experten. Es sei nicht erforderlich, dass die Sicherung gerade gegenüber dem Täter wirkt – wenn dieser etwa ein Administrator ist, der den tatsächlichen Zugriff auf die Daten hat.

Als Überwinden der Zugangssicherung nach § 202a StGB können dem Gericht zufolge auch Handlungen gelten, die nicht besonders anspruchsvoll oder aufwendig sind. Wenn jemand durch Insiderkenntnisse oder Ähnliches eine Absicherung schnell und leicht ausschalten kann, zähle das rechtlich ebenso, als hätte sich jemand durch raffinierte technische Werkzeuge Zugriff verschafft. Nur wenn eine Durchbrechung des Schutzes für jedermann ohne Weiteres möglich sei, werde der Tatbestand nicht erfüllt.

## **Wer den Schaden hat ...**

Wie bereits gesagt, ist strafrechtliche Verfolgung nicht das Einzige, was der illegale Einsatz von Hacking-Tools nach sich ziehen kann: Wenn dabei ein Schaden entsteht, hat der Geschädigte einen Anspruch auf Schadenersatz gegen den Verursacher. Schäden durch IT-Störmanöver können sehr hoch sein – wenn etwa durch den Ausfall von Unternehmensservern Arbeitsprozesse lahmgelegt werden. Auch der Ausfall der Netzkommunikation kann enorme Umsatzeinbußen und damit hohe wirtschaftliche Schäden bedeuten. Für Anspruchsteller im Zivilrecht ist wichtig, dass jede Streitpartei alles, was für ihre Sache spricht, selbst gerichtsfest beweisen muss. Das kann bei Schäden durch Hackertools etwa den Nachweis eines Hackerangriffs und die zweifelsfreie Benennung des Angreifers betreffen. Außerdem ist auch nachzuweisen, dass der Angriff tatsächlich den geltend gemachten Schaden hervorgerufen hat.

Wenn ein Täter bereits strafrechtlich wegen einer Computerstraftat zulasten eines Geschädigten verurteilt worden ist, hat jener es anschließend vergleichsweise leicht, seine Ansprüche gegen den Verurteilten zivilrechtlich geltend zu machen: Das Urteil des Strafgerichts hat selbst bereits

Indizwirkung, zudem kann der Kläger die im Strafverfahren erhobenen Beweise zu seinen Gunsten nutzen.

Ein dritter, bislang noch nicht genannter Bereich, der durch unrechtmäßigen Einsatz von Hackertools berührt werden kann, ist der Datenschutz. Wo bei einem Angriff personenbezogene Daten im Spiel sind, geht es nicht bloß um wirtschaftliche Schäden, sondern möglicherweise auch um die massenhafte Verletzung des informationellen Selbstbestimmungsrechts der Betroffenen. Wer es also als Pentester mit realen Datenbeständen zu tun hat, tut gut daran, die Bestimmungen der europäischen Datenschutzgrundverordnung (DSGVO) sorgfältig zu beachten. ([psz@ct.de](mailto:psz@ct.de))

1. Literatur
2. [Ronald Eikenberg, David Wischnjak, Böse und billig: Hacking-Gadgets, Gefahr durch angriffslustige Hardware, c't 18/2017, S. 62 und S. 64](#)
3. [Verena Ehrl, Elektronische Übeltäter, Rechtliche Aspekte im Zusammenhang mit Spionage- und Sabotage-Gadgets, c't 18/2017, S. 78](#)
4. [Verordnung \(EU\) 2021/821 des Europäischen Parlaments und des Rates vom 20.5.2021 über eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung, der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck: \[heise.de/s/N76o\]\(https://heise.de/s/N76o\)](#)
5. [BGH, Beschluss vom 8.4.2021, Az. 1 StR 78/21: \[heise.de/s/rmDJ\]\(https://heise.de/s/rmDJ\)](#)
6. [LAG Baden-Württemberg, Urteil vom 17.9.2020, Az. 17 Sa 8/20: \[heise.de/s/MXBL\]\(https://heise.de/s/MXBL\)](#)
7. [BGH, Beschluss vom 13.5.2020, Az. 5 StR 614/19: \[heise.de/s/Zvpw\]\(https://heise.de/s/Zvpw\)](#)