Elektronische Übeltäter

Rechtliche Aspekte im Zusammenhang mit Spionage- und Sabotage-Gadgets

Kleine Geräte, die heimlich Hintertüren in Computern einrichten, WLAN-Sicherungen übertölpeln oder gar Hardware gezielt zerstören, sind der Albtraums eines System-verantwortlichen. Fiese Gadgets können jedoch auch wertvolle Dienste beim Aufspüren von Schwachstellen in Datennetzen und IT-Systemen leisten. Wer nach der rechtlichen Bewertung fragt, bekommt nicht immer befriedigende Antworten.

Von Verena Ehrl

Es gibt Gegenstände, mit denen man nach deutschem Recht nicht umgehen darf – man darf sie nicht kaufen, einführen, herstellen, besitzen oder verkaufen und erst recht nicht benutzen. Die Liste dieser Gegenstände ist allerdings sehr kurz und es handelt sich samt und sonders um Waffen und einschlägiges Zubehör: vom Wurfstern über den Regenschirm-Degen bis zum Laserpunkt-Zielmarkierer für Gewehre. Kein Wunder, die Liste befindet sich ja auch in einer Anlage zum Waffengesetz [1]. Das heißt aber nicht, dass das deutsche Recht den Einsatz von Gegenständen jeder anderen Art stets wohlwollend betrachten würde – nur ist etwa bei digitalen Spionage- oder Sabotage-Tools die Frage weitaus schwieriger zu beantworten, was genau verboten ist und warum. Dabei können geschickte Hände mit ihnen möglicherweise mehr gezielten Schaden anrichten als mit eher altmodisch anmutenden Schrecknissen von der Tabuliste des Waffengesetzes.

Strafbar oder „nur“ rechtswidrig?

Es kann viele Gründe und Abstufungen geben, warum oder inwieweit man mit Keyloggern, WLAN-Störern oder Killsticks gegen Gesetze verstößt. Schon die Einfuhr eines Produkts in den Bereich der Europäischen Union kann illegal sein. Dasselbe kann für den Handel damit und

die Werbung dafür gelten, natürlich erst recht für die Nutzung des Produkts zu rechtswidrigen Zwecken.

Allerdings hat längst nicht alles, was aus den verschiedensten Gründen illegal ist, auch eine strafrechtliche Bedeutung. Das Strafrecht bedroht gesetzlich verbotenes Verhalten mit staatlichen Sanktionen. Das Zivilrecht hingegen regelt Streitfälle zwischen Privatleuten respektive Unternehmen und kommt dann zum Einsatz, wenn jemand Rechte anderer verletzt oder andere schädigt. Darüber hinaus gibt es noch diverse produktbezogene Bestimmungen, deren Verletzung etwa zollrechtliche Konsequenzen hat.

Straftäter im Visier

Das deutsche Strafrecht hebt vorwiegend auf den Taterfolg ab – also auf das Ergebnis, zu dem eine Tat führt. Bei allen Tatbeständen, die mit Daten zu tun haben, ist das üblicherweise die Störung der rechtmäßigen Verfügungsgewalt über die Daten. Auch im Zusammenhang mit elektronischen Hilfsmitteln geht es hier also um das Ergebnis einer kriminellen Nutzung.

Ziemlich klar ist das bei Killer-USB-Sticks: Wer damit nur eigene Hardware röstet, macht sich nicht strafbar. Anderenfalls geht es um eine Sachbeschädigung nach Paragraf 303 des Strafgesetzbuchs (StGB). Unerheblich ist, ob der Täter das beschädigte Objekt wieder ersetzen und den Schaden damit beheben kann. Es ist auch nicht entscheidend, ob der Gegenstand ganz oder nur teilweise zerstört wurde.

Daten hingegen sind keine körperlichen Gegenstände, § 303 StGB greift somit nicht. Der Gesetzgeber musste darauf reagieren und hat § 303 a und b ins StGB eingefügt: Damit wird die Veränderung und Zerstörung von Daten unter Strafe gestellt.

Daten im Sinne des Gesetzes sind nach § 202a Abs. 2 StGB nur solche, die elektronisch, magnetisch oder in anderer nicht unmittelbar wahrnehmbarer Form gespeichert sind oder übermittelt werden. Betroffen sind zudem nur solche Daten, an denen ausschließlich jemand anderem das Recht zur Veränderung, Nutzung und Löschung zusteht. Damit fallen beispielsweise Arbeitnehmer, die von ihrem Job her mit den Daten arbeiten dürfen, aus der Strafbarkeit heraus. Sie können durch unerlaubte Veränderung oder Löschung von Daten jedoch heftigen zivilrechtlichen Ärger bekommen, der sich beispielsweise in Schadenersatzansprüchen äußert.

Die strafbare Datenveränderung erfasst alles, was den Zugriff des Berechtigten erschwert oder unmöglich macht, also etwa Unterdrücken, Löschen, Unbrauchbarmachen und Abändern. Dabei ist es egal, ob der Täter die Daten etwa durch Überschreiben löscht oder das Speichermedium, auf dem sie sich befinden, physisch zerstört.

Computersabotage

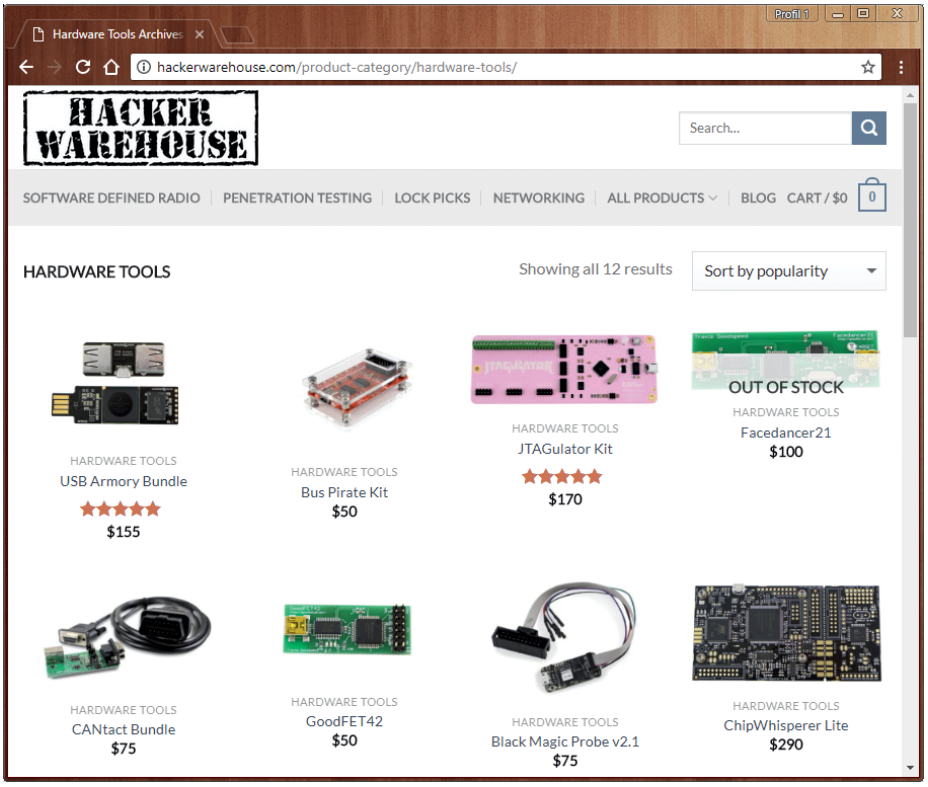
§ 303b StGB stellt unter bestimmten Bedingungen die Störung von Datenverarbeitungsvorgängen unter eine höhere Strafe. Das gilt etwa dann, wenn ein Geschädigter auf die Funktionsfähigkeit der Datenverarbeitung angewiesen ist. Hiervon sind Vorgänge in Unternehmen betroffen, aber auch im privaten Bereich. Wann die Bedeutung für einen Geschädigten wesentlich ist, hängt vom Einzelfall ab.

Damit die Strafbestimmung über Computersabotage greift, braucht noch nicht einmal ein konkreter Schaden eingetreten zu sein – es genügt schon, dass der Täter die Gefahr dafür schafft. § 303 Abs. 2 erfasst die missbräuchliche Eingabe und Übermittlung von Daten, die in der Absicht geschieht, jemandem einen Nachteil zuzufügen. Ein solcher Nachteil kann, muss aber nicht unbedingt ein Vermögensschaden sein. Ein klassisches Beispiel in diesem Zusammenhang sind Denial-of-Service-Angriffe (DoS). Auch der Einsatz von Spionagegadgets kann hier erfasst sein, wenn etwa das Aufzeichnen von Bildern ohne Kenntnis und Einwilligung eines Betroffenen geschieht und dieser dann durch den Upload des Materials in Social Networks lächerlich gemacht wird.

§ 303 Abs. 3 schließlich stellt auf die Zerstörung der Hardware ab. Vom Magneten bis zum explodierenden USB-Stick können hier die verschiedensten Hilfsmittel als Tatwerkzeuge eine Rolle spielen.

Tausend Augen

Auch abseits dieser speziellen Strafrechtsparagrafen gibt es technische Vorgänge, die zu einem kriminellen Ergebnis führen. Als Beispiel kann der Einsatz der GSM-Wanze dienen – im Kern ist das ein primitives Handy mit SIM- und MicroSD-Karte, das lauscht und speichert. Damit kann man wunderbar etwa die verwaiste Gartenlaube überwachen, wenn man im Urlaub ist. Es lässt sich aber auch benutzen, um Mitmenschen heimlich zu belauschen.



Das „Hacker Warehouse“ ist ein Eldorado für Experimentierer, aber auch für Leute mit finsteren Absichten. Der Online-Shop gehört zur Godai Group, einer in Kalifornien beheimateten Unternehmensgruppe mit Schwerpunkt auf Werkzeugen, Diensten und Informationen rund um IT- und Netzsicherheit.

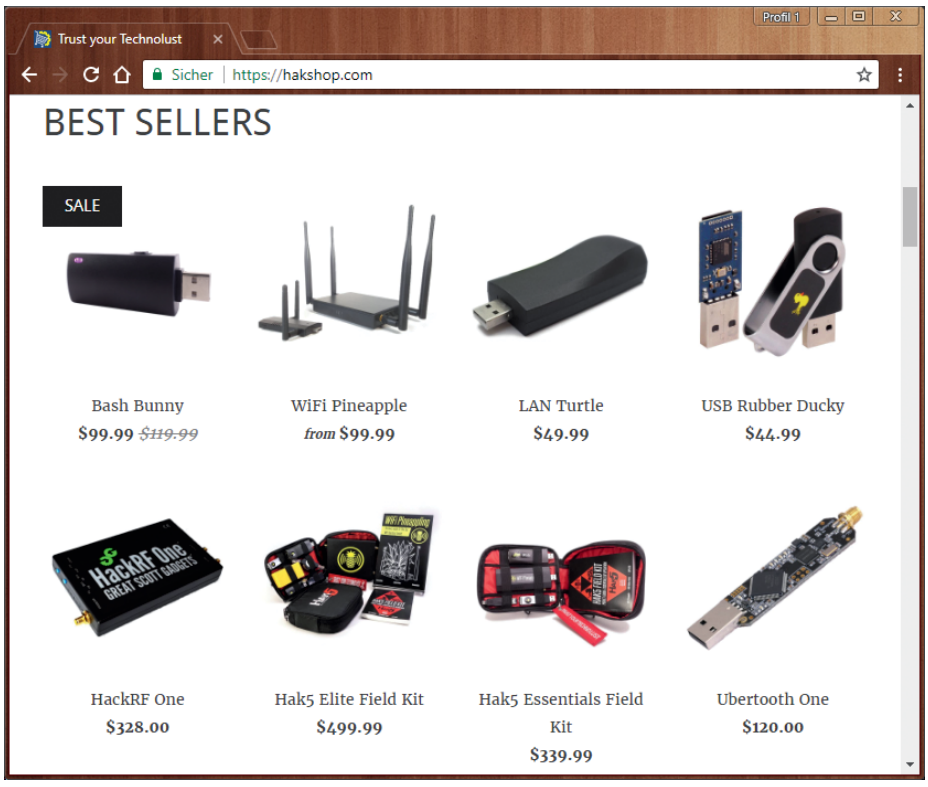
Grundsätzlich unzulässig ist die Überwachung öffentlicher Räume – das betrifft visuelle Information ebenso wie akustische. Wenn es etwa um Kameras geht, müssen diese so eingestellt werden, dass sie ausschließlich das eigene Grundstück beziehungsweise Haus erfassen. Gehwege, Straßen, Grundstücke des Nachbarn, sogar gemeinsame Zufahrten sind tabu. Unzulässig ist bereits, auch nur – etwa mit Attrappen – den Anschein zu erwecken, dass diese Bereiche überwacht werden.

§ 201 StGB stellt die Vertraulichkeit des Wortes unter den Schutz des Strafgesetzes, § 201a betrifft Bildaufnahmen. Sobald ein Gerät in der Lage ist, Gespräche aufzuzeichnen, riskiert ein Verwender bereits, sich strafbar zu machen. Geschützt ist insbesondere das nicht öffentlich gesprochene Wort – rechtswidrig ist somit die Überwachung von Telefonaten und vertraulichen direkten Gesprächen, unabhängig davon, ob der Überwachende selbst Teilnehmer eines solchen Gesprächs ist oder nicht.

Selbst wenn keine Aufnahmen gemacht werden, sondern nur eine heimliche Übertragung stattfindet, werden dabei Persönlichkeitsrechte der Belauschten verletzt.

Der legale Einsatz eines Überwachungsgeräts ist mit Pflichten für den Nutzer verbunden: Ein deutliches Hinweisschild muss etwa Besucher vor dem Betreten überwachter Räume auf die Überwachung aufmerksam machen. Die Aufzeichnungen aus den Geräten dürfen nur für einen begrenzten Zeitraum gespeichert werden, dann sind sie zu löschen. Automatisch angefertigte Bilder, etwa bei einem Einbruch, darf man keineswegs im Zuge einer Do-it-yourself-Fahndung ins Netz stellen.

Bei Fotos oder Videos, die im Netz landen, können auch Straftatbestände aus dem Kunsturheberrechtsgesetz (KUrhG) berührt sein: § 22 und 23 stellen die Verbreitung oder das öffentliche Zurschaustellen eines Bildnisses ohne Einwilligung des Abgebildeten unter Strafe. Auch wenn man sich nicht strafbar gemacht hat, kann ein Aufgenommener dennoch zivilrechtliche Ansprüche stellen. Je nach Umständen des Falles können die von der Vernichtung der Aufzeichnungen über die Unterlassung weiterer Aufnahmen (was die Demontage der Aufzeichnungsgeräte bedeutet) bis hin zu Schadenersatz und Schmerzensgeld reichen.



In seinem „Hakshop“ bietet das kalifornische Hak5-Team Equipment aus eigener Entwicklung, das zum Eindringen in Netze, zum Spionieren und Stören geeignet ist. Dazu gehört der beliebte „Bash Bunny“, der eine Fülle unterschiedlicher Angriffe auf einen angeschlossenen Computer durchführen kann.

Datenleck Marke Eigenbau

Zu den besonders wirkungsvollen elektronischen Datenspionen gehören Keylogger, die jede Aktivität an der Computertastatur aufzeichnen. Es gibt sie in reiner Software-Form als zu installierende und unauffällig im Hintergrund mitlaufende Protokollierungsprogramme. Praktischer in der Anwendung sind USB-Keylogger in Form harmlos aussehender USB-Sticks, die gleich einen eigenen Speicher mitbringen. Sie sind als gar nicht heimliche Helfer bei IT-Supportern beliebt, weil man damit gut Eingabefehlern von Benutzern auf die Spur kommen und unkompliziert ein Backup von Texteingaben anfertigen kann. Andererseits lassen sie sich auch gut zur Überwachung und zum Ausspionieren nutzen. Heimlich eingesetzt offenbaren sie dem Unbefugten Passwörter, Anwender-Logins und vieles mehr.

Für arbeitsrechtliches Aufsehen hat Ende Juli der Fall eines angestellten Web-Entwicklers gesorgt, der seinen Dienstrechner pflichtwidrig auch für private Zwecke genutzt hatte und mit Hilfe eines heimlich installierten Keyloggers überführt worden war. Das Bundesarbeitsgericht (BAG) verbot die Verwertung der Keylogger-Aufzeichnungen in diesem Fall [2]: Der Einsatz eines solchen Werkzeugs für eine verdeckte Überwachung und Kontrolle des Arbeitnehmers ist nach § 32 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) unzulässig, wenn damit nicht ein durch konkrete Tatsachen begründeter Verdacht einer Straftat oder einer anderen schwerwiegenden Pflichtverletzung verifiziert werden soll.

Wie bei vielen anderen Werkzeugen zum Überwachen und Protokollieren ist auch beim Keylogger weder Kauf noch Besitz strafbar – sehr wohl kann sich aber jemand durch den Einsatz eines solchen Geräts strafbar machen, wenn er etwa Geschäftsgeheimnisse stiehlt oder mithilfe der Keylogger-Daten einen Betrug begeht.

Sobald ein Keylogger personenbezogene oder -beziehbare Daten abschöpft, wird es auch datenschutzrechtlich kritisch: Das Bundesdatenschutzgesetz (BDSG) verbietet es in § 43 Abs. 2, unbefugt personenbezogene Daten zu beschaffen, zu erheben, zu verarbeiten oder solche Daten zweckentfremdet zu nutzen. Voraussetzung ist jeweils, dass es sich nicht um allgemein zugängliche Daten handelt. Bei § 44 BDSG geht es dann nicht mehr um eine Ordnungswidrigkeit, sondern um eine Straftat: nämlich dann, wenn eine

Schädigungs- oder Bereicherungsabsicht vorliegt.

Der Reiz fremder Funkwellen

Eine beliebte Freizeitbeschäftigung für den geneigten Hobby-Hacker ist das Aufspüren und Nutzen offener WLAN-Verbindungen. Wer verschlüsselte WLAN-Kommunikation knackt, kann sich auf verschiedene Weise strafbar machen – auch wenn er zum Knacken keine eigene Intelligenz einsetzt, sondern lediglich einen elektronischen WLAN-Überlister. § 202 a–c StGB umfasst den unbefugten Zugang zu besonders gesicherten Daten durch Hacking sowie die Vorbereitung dazu. Mehr zu diesem sogenannten Hackerparagrafen sagt der Kasten rechts.

Selbst das Mitlesen unverschlüsselter WLAN-Kommunikation ist nach § 89 und 148 des Telekommunikationsgesetzes (TKG) strafbar. Diese Vorschriften verbieten das Abhören von Nachrichten, die über eine Funkanlage gesendet werden. Es gibt bisher nur wenig Rechtsprechung dazu, daher ist die Thematik immer noch umstritten. Das Landgericht (LG) Wuppertal hat 2010 entschieden, dass zumindest das bloße unbefugte Surfen unter Verwendung eines fremden offenen WLAN nicht strafbar ist [3]. Etwas anderes dürfte aber gelten, wenn Daten gezielt abgefangen und ausgelesen werden; § 89 TKG bietet dafür genügend Spielraum.

Du kommst hier nicht rein!

In Konflikt mit dem Gesetz kann man durch elektronische Gadgets auch auf ganz andere Weise geraten als bisher gezeigt – nämlich durch deren illegale Einfuhr in den Handelsraum der Europäischen Union. Hier geht es um Ordnungswidrigkeiten, die mit Geldbußen geahndet werden. Es kann auch sein, dass Geräte, die jemand rechtswidrig importieren will, vom Zoll beschlagnahmt und vernichtet werden. Bei Gadgets, die mit Funktechnik arbeiten, ist beispielsweise wichtig, dass sie den Bestimmungen des Gesetzes über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) entsprechen. Auch die Vorschriften des Produktsicherheitsgesetzes (ProdSG) samt der dazugehörigen Verordnungen müssen erfüllt sein.

Seit Mai 1985 muss für Produkte, die im Bereich der EU in Verkehr gebracht werden, außerdem eine Erklärung des Herstellers darüber vorliegen, dass das Produkt sämtlichen aktuell anwendbaren europäischen Richtlinien entspricht. Dies dokumentiert der Hersteller oder sein im EU-Gebiet ansässiger Bevollmächtigter, indem er die CE-Kennzeichnung auf das Produkt aufbringt. Ohne eine solche Konformitätskennzeichnung dürfen Produkte, auf die die einschlägigen Richtlinien anzuwenden sind, in der EU nicht in Verkehr gebracht und auch nicht in Betrieb genommen werden.

Interessanterweise finden sich unter den Richtlinien, die das betrifft, mindestens zwei, die für elektronische Geräte relevant sind: 89/336/EWG über elektromagnetische Verträglichkeit und 91/263/EWG über Telekommunikationsendeinrichtungen.

Der Zoll informiert auf seiner Website www.zoll.de darüber, welche Vorschriften für die Einfuhr von Produkten in den EU-Raum gelten. Es lohnt sich, ein wenig Zeit für diese etwas sperrige Lektüre aufzubringen, wenn man in Bezug auf den Einsatz importierter Gadgets rechtlich auf der sicheren Seite sein will. *(psz@ct.de)* c't

Literatur

[1] Verbotene Gegenstände: Anlage 2 zu § 2 Abs. 2 bis 4 des Waffengesetzes (WaffG)
[2] BAG, Urteil vom 27. 7. 2017, Az. 2 AZR 681/16
[3] LG Wuppertal, Beschluss vom 19. 10. 2010, Az. 25 Qs 177/10
[4] BVerfG, Beschluss vom 18. 5. 2009, Az. 2 BvR 2233/07, 1151/08 und 1524/08

Entscheidungen: ***ct.de/y3qp***

Der berüchtigte „Hackerparagraf“

Seit 2007 befindet sich im deutschen Strafgesetzbuch (StGB) der Paragraf 202 c, der die Beschaffung, Verbreitung, Überlassung und den Verkauf von Zugangscodes und Passwörtern für den unbefugten Zugriff auf gesicherte fremde Daten unter Strafe stellt. Dasselbe gilt für Herstellung, Zugänglichmachung und so weiter von Computerprogrammen, die einem solchen Zweck dienen. Es geht dabei um die Vorbereitung einer Straftat, nämlich des Ausspähens (§ 202a StGB) oder des Abfangens (§ 202b) von Daten, und es drohen Freiheitsstrafen bis zu zwei Jahren oder zumindest eine Geldstrafe.

Ähnlich wie beim Geldfälschen entgeht der Vorbereitende der Strafe, wenn er die Sache aufgibt, eine durch die Vorbereitung heraufbeschworene Gefahr abwendet oder die Vollendung der vorbereiteten Tat aktiv verhindert. Die Software-Werkzeuge, um die es geht, muss er vernichten, unbrauchbar machen oder sie den Behörden offenlegen respektive überlassen.

Dieser sogenannte Hackerparagraf ist seit seiner Einführung hoch umstritten – insbesondere weil der Gesetzgeber nicht geklärt hat, was man unter dem Begriff „Computerprogramme, deren Zweck die Begehung einer solchen Tat ist“, konkret verstehen soll. Wer die Bestimmung restriktiv auslegt, lässt sämtliche Software-Werkzeuge zum Aufspüren von Sicherheitslücken darunter fallen, ungeachtet dessen, ob diese ebenso gut legalen Zwecken dienen können oder nicht. Ein zentraler Streitpunkt ist von Beginn an die Frage gewesen, welche Konsequenz der „Dual Use“ eines Werkzeugs hat – also der Umstand, dass dieses eben mehrerlei Zwecken dienen kann, die keineswegs alle die Vorbereitung von Straftaten betreffen. Eine ausdrückliche Ausnahmeregelung für Werkzeuge zum Penetration Testing sieht der Wortlaut des Gesetzes nicht vor.

2009 stellte das Bundesverfassungsgericht (BVerfG) klar, die Bestimmung beziehe sich ausschließlich auf solche Tools, die dediziert auf einen kriminellen Zweck abzielen und so bereits mit illegaler Absicht hergestellt wurden [4]. Die viel diskutierten „Dual Use“-Produkte seien davon nicht erfasst – zumindest fehle demjenigen, der solche Software zu legalen Zwecken nutze, der für eine Strafbarkeit notwendige Vorsatz.

Ein zusätzliches Problem liegt in der Einschränkung des Gesetzeswortlauts auf „Computerprogramme“. Streng genommen würden reine Hardware-Lösungen nicht davon erfasst, was aber nicht der Absicht des Gesetzgebers entspricht.