Strafrechtschutz für IT und Daten

Antonia Herfurth, Juristin in München

APRIL 2015

„Die Wirtschaft steht an der Schwelle zu einer vierten industriellen Revolution. Dabei wachsen die reale und virtuelle Welt immer mehr zu einem Internet der Dinge zusammen." Durch die Entwicklung zu einer digitalen Wirtschaft, gewinnt insbesondere die Informationssicherheit an Bedeutung. Diese kann als Schutz von technischen Systemen vor Angriffen und Missbrauch verstanden werden. Kleine und mittelständische Unternehmen fürchten in diesem Zusammenhang um die Sicherheit ihrer Betriebsdaten und den Verlust von Geschäftsgeheimnissen.

Tatsächlich ergeben sich durch die aktuellen technischen Entwicklungen mehr Tatgelegenheiten und neue Tatgelegenheitsstrukturen. So wurden im Jahr 2014 in Deutschland etwa 50.000 Straftaten im Bereich Cybercrime begangen und dabei Schäden in Höhe von circa 39 Mio. Euro verursacht. Hierbei ist von einem großen Dunkelfeld auszugehen. Eine Studie aus dem Jahr 2013 hat beispielsweise in Niedersachsen eine Dunkelziffer von 91 % errechnet.

Eine Hürde der Strafverfolgung ist, dass viele der durch Computerkriminalität verletzten Rechtsnormen Antragsdelikte sind. Strafverfolgungsvoraussetzung ist somit grundsätzlich ein Antrag bei den Strafverfolgungsbehörden durch das betroffene Unternehmen. Erschwerend tritt hinzu, dass das Unternehmen in

dem Moment, in dem es staatliche Hilfe in Anspruch nimmt, die Kontrolle über das Verfahren verliert. Denn Staatsanwaltschaft und Gericht sind im Strafprozess von Amts wegen verpflichtet das wirkliche Geschehen zu erforschen und aufzuklären. Somit kann ein Unternehmen durch die Ermittlungen zur Wahrheitsfindung auch in ein negatives Licht rücken.

Die folgende Darstellung verschafft einen Überblick über potenziell einschlägige Strafrechtsnormen im Zusammenhang mit der Computerkriminalität.

Übersicht über die Rechtssituation

Als „Motor der Fortentwicklung des Computerstrafrechts" fungierten in der Vergangenheit insbesondere die Europäische Union und der Europarat. Durch die *Cybercrime-Konvention* des Europarates aus dem Jahr 2001 erfolgte eine Harmonisierung der nationalen Strafvorschriften im Bereich der Cyber-Kriminalität. Die Union wirkt mittels Art. 83 Abs. 1 AEUV an der Bekämpfung der Computerkriminalität mit, indem sie „durch Richtlinien Mindestvorschriften zur Festlegung von Straftaten und Strafen in Bereichen besonders schwerer Kriminalität festlegen" kann.

Relevante nationale Strafnormen im Zusammenhang mit dem Angriff auf und Missbrauch von Daten, die nicht personenbezogen sind, finden sich überwiegend im Strafgesetzbuch (StGB), vereinzelt im Gesetz gegen den unlauteren Wettbewerb (UWG). Handelt es sich um eine Verletzung personenbezogener Daten, ist auf Bundesebene insbesondere an das Bundesdatenschutzgesetz zu denken. Der Fokus liegt im Folgenden auf der Darstellung nationaler Normen, deren Ziel der nicht personenbezogene Datenschutz ist, insbesondere unter Betrachtung der Entwicklung Industrie 4.0.

Hierbei können die einschlägigen Normen klassifiziert werden:

- Angriffe gegen Informationssysteme durch das Ausspähen, § 202a StGB, und Abfangen von Daten, § 202b StGB, sowie die Vorbereitung dessen,

§ 202c StGB, die Datenhehlerei, § 202 d StGB, die Datenveränderung, § 303a StGB, und die Computersabotage, § 303b StGB,

- Urkundendelikte wie die Fälschung technischer Aufzeichnungen und beweiserheblicher Daten, §§ 268, 269 StGB, sowie die Urkunden- und Datenunterdrückung, § 274 StGB,

- das Vermögensdelikt des Computerbetrugs, § 263a StGB und

- Angriffe auf Daten- und Geheimnisschutz durch Verrat von Geschäfts- und Betriebsgeheimnissen, § 17 UWG, und Verleiten und Erbieten zum Verrat, § 19 UWG.

Die Straftatbestände

Im Folgenden werden die einzelnen Straftatbestände vorgestellt. Der juristische Aufbau eines vorsätzlich vollendeten Begehungsdelikts gliedert sich in Tatbestand, Rechtswidrigkeit und Schuld, wobei im Rahmen des Tatbestands zwischen objektivem und subjektivem Tatbestand differenziert wird. Der objektive Tatbestand erfasst die tatbestandlichen Voraussetzungen einer Strafrechtsnorm (Täter, Tathandlung, Taterfolg und Ursächlichkeit), wohingegen der subjektive Tatbestand den Vorsatz des Täters thematisiert. Nachfolgend wird schwerpunktmäßig der objektive Tatbestand dargestellt, wohingegen auf die sonstigen Voraussetzungen nur eingegangen wird, sofern sich diesbezüglich Besonderheiten ergeben.

Angriffe gegen Informationssysteme

Computerspionage, „Datendiebstahl“,

§ 202a StGB stellt das Ausspähen von Daten unter Strafe. Dabei schützt die Norm die Verfügungsbefugnis des Berechtigten an dem gedanklichen Inhalt seiner Daten, sprich sein Geheimhaltungsinteresse. Erfasst werden somit insbesondere Fälle der Datenspionage.

Das Tatobjekt „Daten“ ist in § 202a II StGB legal definiert als solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. Voraussetzung ist, dass die Daten nicht für den Täter bestimmt und gegen unberechtigten Zugang besonders gesichert sind. Unternehmen haben an dieser Stelle zu beachten, dass bloße Zugriffsverbote in Verträgen oder etwa das Abspeichern von Daten unter einem anderen Namen oder in einem anderen Verzeichnis keine geeignete Sicherung im Sinne der Norm darstellt. Als geeignete Tathandlung muss der Täter sich oder einem anderen unter Überwindung der Zugangssicherung den Zugang zu Daten verschafft haben.

> Beispiel:
> *Der Täter hackt den Server eines Unternehmens unter Einsatz von Backdoorprogrammen, Netzwerksniffern oder Trojanern.*

§ 202b StGB schützt, ebenso wie § 202a StGB, das Geheimhaltungsinteresse des Berechtigten. Indem es das Abfangen von Daten bestraft, stützt sich der Schutzbereich des § 202b StGB aber nicht auf den Geheimhaltungswillen, sondern auf das allgemeine Recht auf Nichtöffentlichkeit der Kommunikation.

Tatbestandsvoraussetzung ist, dass sich der Täter unter Anwendung von technischen Mitteln Daten i.S.d. § 202a II StGB aus einer nichtöffentlichen elektronischen Datenübermittlung verschafft. Der Tatbestand ist nur erfüllt, wenn sich die Daten zum Tatzeitpunkt im Übermittlungsvorgang befinden, sprich vom Täter „abgefangen“ werden. Eines weiteren Aufzeichnens oder Speicherns der Daten bedarf es zur Erfüllung des § 202b StGB nicht.

> Beispiel:
> *Ein Mitarbeiter sendet eine E-Mail an einen Kunden, die von einem Wettbewerber abgefangen und gelesen wird.*

Begeht der Täter Vorbereitungshandlungen, die als solche bereits besonders gefährlich sind, unterliegt er der Strafbarkeit nach § 202c StGB.

Vorbereitungshandlungen

Strafbar macht sich danach, wer eine Tat nach §§ 202a, 202 b, 303 a oder 303 b StGB vorbereitet, indem er Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht. Als Ausgleich zu der weiten Vorverlagerung der Strafbarkeit wird dem Täter die Möglichkeit der Strafaufhebung aufgrund tätiger

Reue eröffnet. Gibt er also die Ausführung der vorbereiteten Tat freiwillig auf, entfällt seine Strafbarkeit.

> Beispiel:
> *Ein Software-Entwickler kreiert ein Hacking-Programm, das den Zweck hat Daten auf fremden Computern auszuspähen.*

In diesem Bereich entsteht eine praktische Frage, die Systemtester vor Schwierigkeiten stellt: allein der Besitz von Hacker-Software, die zu Testzwecken eingesetzt werden soll, wäre bereist strafbar.

Datenhehlerei

Im Dezember 2015 wurde mit § 202 d StGB ein neuer Straftatbestand eingeführt, die Datenhehlerei. Danach macht sich strafbar, wer Daten, die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Vortat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht. Subjektiv muss der Täter nicht nur vorsätzlich, sondern auch mit Bereicherungsabsicht oder Drittschädigungsabsicht handeln.

> Beispiel:
> *Ein Mitarbeiter eines Unternehmens übernimmt von einem Hacker die bei einem Wettbewerber unbefugt kopierten Kundendaten, um diese Kunden selbst zu gewinnen.*
>
> Anders:
> *Ein Journalist übergibt Daten, die er auf vertraulichem Weg von einem Mitarbeiter als Whistleblower erhalten hat, vertraulich an einen Zeitungsredakteur zur Einschätzung. Dieser überspielt sich die Daten in Form einer Word-Datei auf einen USB-Stick.*

Computersabotage

Ein Angriff auf Informationssysteme kann ebenso durch die Begehung einer Datenveränderung nach § 303a StGB erfolgen. Geschütztes Rechtsgut ist das Interesse des Berechtigten an der unversehrten Verwendbarkeit von Daten.

Auch hier sind alle Daten i.S.d. § 202a II StGB, über die der Täter nicht die alleinige Verfügungsbefugnis besitzt, geeignetes Tatobjekt. Als Tathandlung muss der Täter Daten gelöscht, dem ein Unkenntlichmachen gleichgestellt ist, unterdrückt, unbrauchbar gemacht oder verändert haben.

Im Übrigen ist bereits der Versuch der Datenveränderung strafbar und § 303b StGB, die Computersabotage, stellt eine Qualifikation zu § 303a StGB dar, also eine Erweiterung des Grundtatbestandes um strafverschärfende Merkmale.

> Beispiel:
> *Der Täter überschreibt Kundendaten im fremden Unternehmen, sodass diese unwiederbringlich unkenntlich gemacht sind.*

Geschütztes Rechtsgut der Computersabotage aus § 303b StGB ist „das Interesse der Betreiber und Nutzer von Datenverarbeitungen an deren ordnungsgemäßer Funktionsweise“.

Strafbar ist, wer eine Datenverarbeitung, die wesentliche Bedeutung für den Betroffen hat, erheblich stört. Dies kann durch eine Datenveränderung geschehen, durch Eingeben oder Übermitteln von Daten oder auch durch das Zerstören, Beschädigen, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers. Als Besonderheit muss der Täter bei der Tathandlung des Eingebens oder Übermittelns im subjektiven Tatbestand mit einer Nachteilszufügungsabsicht zu Lasten des Betreibers beziehungsweise Nutzers handeln.

Ferner ist bereits eine versuchte Computersabotage strafbar.

Außerdem enthält § 303b II StGB eine Qualifikation zu § 303b I StGB. Danach wirkt sich strafschärfend aus, wenn die Datenverarbeitung für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung war. Strafschärfung tritt auch bei einer Computersabotage in einem besonders schweren Fall ein, so zum Beispiel, wenn der Täter einen Vermögensverlust großen Ausmaßes herbeigeführt hat.

> Beispiel:
> ein Mitarbeiter *löscht Daten auf dem Unternehmensserver die die Verträge mit wichtigen Kunden enthalten.*

Urkundendelikte

Fälschung technischer Aufzeichnungen

§ 268 StGB bestraft die Fälschung technischer Aufzeichnungen. Somit wird die Sicherheit und Zuverläs-

sigkeit des Rechts- und Beweisverkehrs geschützt und damit das Vertrauen in die technische Informationsgewinnung und die Echtheit technischer Aufzeichnungen.

Tatbestandsvoraussetzung ist, dass der Täter eine unechte technische Aufzeichnung herstellt, eine technische Aufzeichnung verfälscht oder eine unechte oder verfälschte technische Aufzeichnung gebraucht. Der Herstellung einer unechten technischen Aufzeichnung steht es gleich, wenn der Täter durch störende Einwirkung auf den Aufzeichnungsvorgang das Ergebnis der Aufzeichnung beeinflusst. Die technische Aufzeichnung ist in § 268 II StGB legal definiert als eine Darstellung von Daten, Mess- oder Rechenwerten, Zuständen oder Geschehensabläufen, die durch ein technisches Gerät ganz oder zum Teil selbstständig bewirkt wird, den Gegenstand der Aufzeichnung allgemein oder für Eingeweihte erkennen lässt und zum Beweis einer rechtlich erheblichen Tatsache bestimmt ist, gleichviel ob ihr die Bestimmung schon bei der Herstellung oder erst später gegeben wird. Subjektive Voraussetzung des § 268 I StGB ist, das der Täter zur Täuschung im Rechtsverkehr oder aus Gründen der fälschlichen Beeinflussung einer Datenverarbeitung im Rechtsverkehr handelt.

Bereits der Versuch ist strafbar.

Eine höhere Strafe droht, wenn der Täter eine Fälschung technischer Aufzeichnung in einem besonders schweren Fall begangen hat, beispielsweise einen Vermögensverlust besonders großen Ausmaßes herbeigeführt hat.

> Beispiel:
> *Der Fahrer hat in seinem LKW ein digitales EU-Kontrollgerät. Er manipuliert das Gerät so, dass die Geschwindigkeit um 10 km/h zu niedrig aufgezeichnet wird.*

Fälschung beweiserheblicher Daten

§ 269 StGB stellt die Fälschung beweiserheblicher Daten unter Strafe und schützt somit die Sicherheit und Zuverlässigkeit des Rechts- und Beweisverkehrs mit Daten. Zweck der Vorschrift ist die Schließung computerspezifischer Strafbarkeitslücken im Bereich der Urkundendelikte.

Der objektive Tatbestand ist erfüllt, wenn der Täter beweiserhebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht. Daten im Sinne der Norm sind „Informationen, die in einer primär für die maschinelle Verarbeitung bestimmten Form codiert“ und somit „nicht unmittelbar optisch wahrnehmbar“ sind. Aufgrund der Bedeutung des § 269 StGB als „computerspezifisches Urkundendelikt“ müssen die Daten geeignet sein im Rechtsverkehr Beweis für rechtlich erhebliche Tatsachen zu erbringen und aufgrund dessen alle Funktionen einer Urkunde erfüllen, sprich Beweis-, Garantie- und Perpetuierungsfunktion. Daten i.S.d. § 269 StGB sind bereits unecht, wenn sie über die Identität des Ausstellers täuschen, wohingegen bloße inhaltliche Datentäuschungen unerheblich sind. Abschließend ist aufzuzeigen, dass durch die Tathandlung des Speicherns oder Veränderns eine in hypothetischer Hinsicht unechte oder verfälschte Urkunde vorliegen muss. Würde es sich also um ein wahrnehmbares Tatobjekt, eine Urkunde, handeln, müsste diese durch die Tathandlung unecht oder verfälscht worden sein. Subjektiv muss der Täter zur Täuschung im Rechtsverkehr oder aus Gründen der fälschlichen Beeinflussung einer Datenverarbeitung im Rechtsverkehr gehandelt haben.

> Beispiel:
> *Ein Mitarbeiter setzt unbefugt eine fremde Zahlungskarte zur Zahlung von Waren mittels PIN im electronic-cash-Verfahren ein.*

Unterdrückung von Beweismitteln

Schließlich ist § 274 StGB als geeignetes Urkundendelikt im Zusammenhang mit Computerstraftaten anzuführen. Sinn und Zweck der Norm ist, den Bestand der genannten Beweismittel zu gewährleisten um somit mit ihnen Beweis erbringen zu können.
Der Strafbarkeit unterliegt, wer eine echte technische Aufzeichnung i.S.d. § 269 StGB, welche ihm entweder überhaupt nicht oder nicht ausschließlich gehört, vernichtet, beschädigt oder unterdrückt. Ebenso wird bestraft, wer beweiserhebliche Daten i.S.d. § 202a II StGB, über die er nicht oder nicht ausschließlich verfügen darf, löscht, unterdrückt, unbrauchbar macht oder verändert. In subjektiver Hinsicht bedarf es neben dem Vorsatz stets einer Nachteilszufügungsabsicht des Täters. Diese muss zum einen auf die Beeinträchtigung fremder Rechte gerichtet sein und zum anderen auf eine Beeinträchtigung des Beweisführungsrechts.

Beispiel:
Ein Mitarbeiter löscht eine Datei mit einer Mängelrüge eines Kunden

Vermögensdelikte

Computerbetrug

§ 263a StGB bestraft den Computerbetrug, indem der Täter durch Manipulation des Computers, dieses zu einem falschen Vorgang veranlasst. Geschütztes Rechtsgut ist das Vermögen. Geeignetes Tatobjekt des Computerbetrugs ist das Ergebnis eines elektronischen Datenverarbeitungsvorgangs, wobei der Begriff der Daten, als alle codierten und codierbaren Informationen, weit gefasst ist. Als Tathandlung muss der Täter das Ergebnis durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst haben. Zur Tatbestandsverwirklichung muss dem Betroffenen durch die Beeinflussung des Datenverarbeitungsvorgangs ein Vermögensschaden entstanden sein. Subjektive Tatbestandsvoraussetzung ist, dass der Täter neben Vorsatz mit Bereicherungsabsicht gehandelt hat.

Bereits die versuchte Computersabotage ist unter Strafe gestellt, ebenso wie bestimmte, für sich bereits gefährliche, Vorbereitungshandlungen. Zuletzt kann sich ein besonders schwerer Fall strafschärfend zu Lasten des Täters auswirken, so zum Beispiel, wenn der Täter einen Vermögensverlust großen Ausmaßes herbeigeführt hat.

Beispiel:
Der Täter verschafft sich illegal Kenntnisse über diejenigen Programme, die Zahlungsvorgänge im Unternehmen steuern. Mithilfe dieser Kenntnisse setzt er zum richtigen Zeitpunkt eine automatische Überweisung auf sein eigenes Konto in Gang.

Daten- und Geheimnisschutz

Verrat von Geschäftsgeheimnissen

§ 17 UWG schützt den Inhaber eines Unternehmens vor Verrat von Geschäfts- und Betriebsgeheimnissen. Im Übrigen schützt es das Interesse der Allgemeinheit an einem unverfälschten Wettbewerb.

Die Norm erfasst drei Fallkonstellationen: den Geheimnisverrat, die Betriebsspionage und die Geheimnisverwertung bzw. –hehlerei. Geheimnisverrat liegt vor, wenn eine bei einem Unternehmen beschäftigte Person ein Geschäfts- oder Betriebsgeheimnis, das ihr im Rahmen des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemanden mitteilt. Um einen Fall der Betriebsspionage handelt es sich, wenn der Täter sich ein Geschäfts- oder Betriebsgeheimnis durch Anwendung technischer Mittel, Herstellung einer verkörperten Wiedergabe des Geheimnisses oder Wegnahme einer Sache, in der das Geheimnis verkörpert ist, unbefugt verschafft oder sichert. Für eine Geheimnisverwertung bzw. –hehlerei müsste der Täter ein Geheimnis durch Geheimnisverrat oder Betriebsspionage erlangt, sich sonst unbefugt verschafft, gesichert, unbefugt verwertet oder jemandem mitgeteilt haben. Neben den objektiven Merkmalen muss der Täter subjektiv zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, gehandelt haben. Zu beachten ist, dass sowohl bei der Betriebsspionage als auch der Geheimnishehlerei jeder Täter sein kann, es bedarf also, im Gegensatz zum Geheimnisverrat, keiner Beziehung des Täters zum Unternehmen.

Bereits der Versuch und das Verleiten und Erbieten zum Verrat sind strafbar.

Beispiel:
Ein *Unternehmen stellt Getränke her. Bei der Herstellung wendet es eine bestimmte Rezeptur an. Die Rezeptur ist an sich bekannt, jedoch ist geheim, dass das Unternehmen von diesem Verfahren Gebrauch macht. Ein Mitarbeiter trägt dieses Geheimnis nach außen.*

Fazit

Im Zusammenhang mit Computerkriminalität wird in Fachkreisen kritisiert, dass das moderne Strafrecht kein Strafrecht zum Schutz der Wirtschaft sei. Es wird angeführt, dass die einschlägigen nationalen Normen hinter dem aktuellen technischen Entwicklungsstand zurückbleiben. Die einschlägigen Straftatbestände erfuhren zwar durch das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität 2007 erhebliche Änderungen, seither erfolgten auf nationaler Ebene jedoch keine bedeutsamen normativen Fortschritte.

Auch die internationale Kooperation ist ein guter Ansatz, befindet sich jedoch noch in den Anfängen. So wurde mit der Cybercrime-Konvention ein wichtiger Schritt getan, dieser allerdings bereits vor 15 Jahren. Gemessen am technischen und industriellen Entwicklungsstand wird diese (Nicht-)Entwicklung den Anforderungen derzeit kaum gerecht. Zumal die Informationssicherheit auch in Zukunft nicht in seiner Komplexität nachgeben wird - proportional zum technischen Fortschritt entwickeln sich auch die Methoden der Täter.

Dies nutzte die Bundesregierung als Handlungsanstoß und verabschiedete im Jahr 2015 das sog. *IT-Sicherheitsgesetz*. Zweck ist die Erhöhung der Sicherheit informationstechnischer Systeme. Das IT-Gesetz stellt dazu branchenspezifische Sicherheitsmindestanforderungen an Unternehmen.

Im Übrigen verfasste die Bundesregierung bereits im Jahr 2014 die *Digitale Agenda 2014-2017*, in der sie Grundsätze zur Digitalpolitik formuliert hat. Dabei misst sie Politikfeldern wie der digitalen Wirtschaft oder Infrastruktur digitales Entwicklungspotenzial zu und versucht dieses durch vorgeschlagene Innovationsstrategien zu unterstützen und voranzutreiben.

Allerdings werden sowohl das IT-Gesetz als auch die Digitale Agenda vielfach als ungenügend kritisiert. Es wird angeführt, dass das IT-Gesetz unzureichend und realitätsfern ausgestaltet sei und die Digitale Agenda lediglich leere Phrasen enthalte, „die (zudem) zehn Jahre zu spät […] vorgelegt“ wurden.

Somit bleibt abzuwarten, wie sich der Gesetzgeber des Weiteren verhält und ob er in der Unzufriedenheit in Fachkreisen über den unzulänglichen Rechtsschutz im Bereich der Computerkriminalität nicht möglicherweise einen Impuls für weitere Maßnahmen sieht.

In der Gesamtbetrachtung - und insbesondere unter den Gesichtspunkten der Entwicklung zu Industrie 4.0 – lässt sich feststellen, dass das nationale Computerstrafrecht nur bedingt geeignet ist, einen effektiven Vermögensschutz von Unternehmen zu gewährleisten. Die Bekämpfung von Wirtschaftskriminalität leidet nicht an einem Regelungsdefizit, sondern an einem Vollzugsdefizit. Die Angriffe erfolgen eben in der Regel nicht durch den benachbarten Wettbewerber, sondern durch internationale Täterstrukturen. Diese können von privaten Tätern, von Wettbewerbsunternehmen oder von staatlichen Stellen ausgehen. Internationale Cyberkriminalität lässt sich aber nur sehr schwer ermitteln und im erfolgreichen Ermittlungsfall ebenso schwer im Ausland verfolgen.

Unternehmen sind daher gut beraten, wenn sie sich technische und organisatorische Schutzmaßnahmen konzentrieren und sich nicht auf eine Abschreckung oder Ahndung durch das Strafrecht verlassen.

+++

compact.
HERFURTH & PARTNER RECHT INTERNATIONAL.

caston.info

Beiträge zu Recht & Wirtschaft International finden Sie kostenfrei im Internet bei caston.info. Unsere Titelliste erhalten Sie auch per Mail.

IMPRESSUM

HERAUSGEBER

HERFURTH & PARTNER Rechtsanwaltsgesellschaft mbH
Luisenstr. 5, D-30159 Hannover
Fon 0511-30756-0 Fax 0511-30756-10
Mail info@herfurth.de, Web www.herfurth.de

Hannover · Göttingen · Brüssel
Member of the ALLIURIS GROUP, Brussels

REDAKTION

KORRESPONDENTEN

u.a. Amsterdam, Athen, Barcelona, Brüssel, Budapest, Bukarest, Helsinki, Istanbul, Kiew, Kopenhagen, Lissabon, London, Luxemburg, Lyon, Mailand, Madrid, Moskau, Oslo, Paris, Prag, Sofia, Stockholm, Warschau, Wien, Salzburg, Zug, New York, Toronto, Mexico City, Sao Paulo, Buenos Aires, Dubai, Kairo, New Delhi, Bangkok, Singapur, Peking, Shanghai, Tokio, Sydney, Johannesburg

VERLAG

CASTON GmbH, Law & Business Information
Luisenstr. 5, D-30159 Hannover,
Fon 0511 - 30756-50 Fax 0511 - 30756-60
Mail info@caston.info Web www.caston.info

compact.
HERFURTH & PARTNER RECHT INTERNATIONAL.

NEUERSCHEINUNG

Industrie 4.0 im Rechtsrahmen
Recht für die digitale Unternehmenspraxis

Industrie 4.0 ist für die meisten Unternehmen nicht mehr nur ein Schlagwort, sondern als Weg in die Digitalisierung von Produktion und Geschäftsprozessen bereits Realität.

Bei der Umsetzung der technologischen Entwicklungen entstehen allerdings zahlreiche neue rechtliche Fragen, die ein Unternehmen geklärt haben muss, um seine Ziele störungsfrei und sicher verfolgen zu können. Im Vordergrund steht die Sicherheit von Prozessen und Produkten - von größter Bedeutung ist aber auch der Umgang mit eigenen und fremden Daten und die Rechte daran. Je mehr sich ein Unternehmen digitalisiert, umso stärker verlagern sich seine Werte in diesem Bereich.

Der neue Report „Industrie 4.0 im Rechtsrahmen“ beschreibt in den verschiedenen Feldern, welche rechtlichen Rahmenbedingungen die Unternehmensprozesse steuern:

Besondere Herausforderungen entstehen aus dem Umgang mit autonomen Prozessen in der Leistungskette, im Qualitätsmanagement, in unternehmens- und in länderübergreifenden Beziehungen und Abläufen. Generierung, Besitz, Verwendung und Verwertung der großen Datenmengen werfen neue Fragen zu Schutz und Zugriffsrechten auf – und verlangen eine privatrechtliche vertragliche Gestaltung. Industrie 4.0 berührt aber auch wichtige andere Bereiche wie Personal und Arbeitsgestaltung, Wettbewerbsrecht, Finanzierung und Rechnungswesen und Beziehungen zu Providern, Plattformen und Netzen.
„Industrie 4.0 im Rechtsrahmen“ greift diese Fragen auf und gibt dazu aktuelle Lösungsansätze.

Industrie 4.0 im Rechtsrahmen
Leistungen, Daten, Strukturen

Herfurth, Ulrich (Hrsg)
Caston Edition, Hannover
ISBN 978-3-936647-03-7

Verlag:
Caston GmbH
Law & Business Information
D-30159 Hannover
Luisenstrasse 5
www.caston.info