Angriff von innen

Vor Angriffen auf IT-Systeme von aussen sind die meisten Unternehmen recht gut geschützt. Doch oft kommen die Täter aus den eigenen Reihen. Diese vor einer Straftat zu erkennen, ist oft schwierig, und die Mittel zur Strafverfolgung sind begrenzt. → VON SUSANN KLOSSEK

Der Fall des Schweizer Unternehmers Peter K. (Name der Redaktion bekannt) liest sich wie das Script zum neusten Spionagethriller und ist doch Realität: Der ehemalige CEO eines Software-Unternehmens musste trotz grossen Erfolgs Konkurs anmelden und steht nun vor den Trümmern seiner Arbeit. Sein einziger Fehler: Er hat seinen Mitarbeitern vertraut. Eine kleine Gruppe aus der Entwicklercrew hat sich den selbst entwickelten Code angeeignet, insgeheim eine eigene Firma gegründet und die Software einfach dorthin mitgenommen. K. war nicht nur von heute auf morgen seine Kernmitarbeiter los, die sogar noch weiteres Personal abzogen, sondern er verlor auch das Vertrauen seiner Kunden. Denn ohne Software und fähige Spezialisten konnte er nicht mehr liefern, sein Ruf war ruiniert.

«Es passiert oft, dass Entwickler meinen, die Software, die sie entwickelt haben, gehöre ihnen», sagt der Ex-Firmenchef. Die Gesetze sprechen jedoch eine klare Sprache: Die Software gehört dem Unternehmen. Allerdings – und das ist das grosse Problem – steht hier das Opfer in der Beweispflicht. Bei Software-Diebstahl, was hierzulande relativ häufig vorkommt, muss der Unternehmer nachweisen, dass die Software auch wirklich in seinem Auftrag entwickelt und danach entwendet wurde. Denn erst dann wird die Staatsanwaltschaft aktiv. Wer seine Mitarbeiter nicht vorsorglich permanent überwacht, für den wird es äusserst schwierig, diesen Beweis zu erbringen. Der erwähnte Fall liegt, mit anderen ähnlichen Fällen, seit einem Jahr bei der Staatsanwaltschaft brach, die ohne bewiesenen Tatbestand auch kein Verfahren eröffnet. Viel Zeit für die Täter, den Software-Code zu modifizieren. Das Perfide: Sobald ein gewisser Prozentsatz des Codes verändert wurde, handelt es sich nicht mehr um dasselbe Produkt. Die Chancen für Peter K., an sein Geld zu kommen oder zumindest Recht zu bekommen, stehen daher schlecht.

Kein Wunder, dass der Ex-Unternehmer aus dem Erlebten heute eine radikale Schlussfolgerung zieht: «Man darf keinem jemals das Gefühl geben, er sei unabdingbar. Sei grundsätzlich misstrauisch und zwar auf radikalste Weise.» Der geprellte Firmenchef empfiehlt jedem Firmenbesitzer,

FOTO: PHOTOCASE.COM/ALLZWECK JACK

Alarmanlagen in die Systeme einzubauen, mittels denen man sehen und nachweisen kann, wo Code kopiert oder Daten gelöscht werden. Jeder Chef müsse sicherstellen, dass er jederzeit hundertprozentigen Zugriff auf seinen Source Code habe und dass dieser kompilierbar sowie aktuell ist. Die Mitarbeiter hingegen sollten immer nur ein Stück vom Code zu Gesicht bekommen. «Lass einen Mitarbeiter niemals allein arbeiten. Am besten lässt man zwei Leute zusammenarbeiten, die sich nicht kennen», sagt K.

RISIKOBEWUSSTSEIN GLEICH NULL

Industriespionage, Diebstahl sensibler Daten, Veruntreuung: Der Schaden, den Mitarbeiter weltweit ihren Unternehmen jährlich zufügen, liegt im hohen dreistelligen Milliardenbereich. Längst ist Fraud – auf Deutsch Betrug – zum Sammelbegriff für die unterschiedlichsten «Verbrechen von innen» geworden. Laut einer Studie der Beratungsgesellschaft PricewaterhouseCoopers wurde 2011 jedes zweite deutsche Unternehmen Opfer von Wirtschaftskriminalität. Das Paradoxe daran: Nur jedes fünfte hält es für realistisch, Opfer derartiger Vergehen zu werden. Die Palette der Delikte ist lang und reicht von entwendeten Kundendaten über den Diebstahl wettbewerbsrelevanter Betriebs- und Geschäftsgeheimnisse bis hin zu gestohlenem Quellcode.

Obwohl neben gestohlenem Software-Code besonders der Diebstahl vertraulicher Kundendaten in letzter Zeit in Mode gekommen zu sein scheint, wie die jüngsten Steuer-CD-Fälle eindrücklich dokumentieren, werden die Gefahren, die von den eigenen Mitarbeitern ausgehen, noch viel zu selten ernst genommen. Besonders kleine und mittlere Unternehmen gehen mit Geschäftsinformationen oft fahrlässig um. Einer Untersuchung des Wirtschaftsprüfungsunternehmens KPMG zufolge, mangelt es vor allem inhabergeführten Firmen an Risikobewusstsein, wie der oben erwähnte Fall zeigt. Dabei wird auch in kleineren Unternehmen geklaut und unterschlagen, was das Zeug hält. Laut Experten tauchen in der Statistik nur deshalb mehr Wirtschaftskriminelle in grossen als in kleineren Unternehmen auf, weil Erstere über bessere Kontrollsysteme verfügen. →

GESTOHLEN WERDEN

6%

Business-Pläne*

* Quelle: Symantec (Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property, 2011)

52 %
Betriebsgeheimnisse*

Egal ob mittelständischer Betrieb oder Grosskonzern, ob Manager oder Angestellter: Beim Sicherheitsbewusstsein herrscht nach wie vor ein grosses Manko. Viel zu schnell werden ohne zu zögern und zu hinterfragen Passwörter preisgegeben, Laptops mit wichtigen Daten – oft unverschlüsselt! – im Zug liegengelassen und dergleichen. Laut Marktforscher Dynamic Markets speichern beispielsweise noch immer 92 Prozent der Manager unternehmenskritische Informationen auf ihren Smartphones bzw. auf Mobilgeräten. Arglos arbeiten die mobilen Manager damit dann im öffentlichen Raum an vertraulichen Dokumenten und Firmeninternas. Dem Datenklau via USB-Stick, E-Mail oder Handy steht in vielen Fällen nichts im Weg.

Wie reine Schusseligkeit zu folgeschwerem Datenverlust führen kann, zeigte im September ein Fall aus dem benachbarten Baden-Württemberg: Dort kamen in zwei Kliniken sensible Patientendaten abhanden, weil ein Mitarbeiter den Datenträger auf einen Tisch gelegt und dort vergessen hatte. Kurze Zeit später war der mobile Datenträger mitsamt den Daten von rund 100 000 Personen verschwunden.

Ein weiterer Problembereich ist die Datenlöschung auf ausgemusterten Rechnern und Festplatten, die vielerorts – falls überhaupt – dilettantisch betrieben wird. Die Täter hingegen werden immer dreister: Selbst komplette Datenbankinhalte werden heutzutage gestohlen. Besonders in forschungsintensiven Branchen wie der Halbleiter-, Pharma- oder Autoindustrie ist der Anreiz gross, Informationen wie Baupläne, Rezepturen oder Beschreibungen zu Fertigungstechniken mitgehen zu lassen und an den höchstbietenden Konkurrenten zu verscherbeln.

WER KLAUT WARUM?

Während in der Vergangenheit besonders Mitarbeiter lange Finger machten, die sich in irgendeiner Art und Weise gekränkt, schlecht behandelt oder übervorteilt fühlten, kann man heute mit Datenklau auch richtig Geld machen. Christoph Baumgartner, CEO und Inhaber des Thalwiler IT-Security-Consulting-Unternehmens OneConsult, kennt die Schwachstellen aus der Praxis: «In vielen Fällen braucht es einen Insider, der ganz nah am Geschehen ist.» Das könne sowohl ein Kundenbetreuer als auch ein Mitarbeiter aus der IT-Abteilung selbst sein. Das Verhältnis der Diebe aus der IT und aus anderen Abteilungen schätzt Baumgartner auf 50 zu 50. Anders als etwa Mitarbeiter aus den Fachbereichen, fühlen sich IT-Spezialisten meist weniger dem Unternehmen, sondern den Systemen und Anwendungen verbunden. Sie suchen sich ihre Arbeitgeber oft nach den dort verwendeten Systemen aus – und umgekehrt.

Ein Fall, bei dem der Datendieb im Informatikbereich gearbeitet hat, wurde Ende September publik (Computerworld berichtete → **Webcode: 61318**). So soll ein Mitarbeiter des Nachrichtendienstes des Bundes im grossen Umfang Daten gestohlen und versucht haben, diese ins Ausland zu verkaufen. Offensichtlich war es ihm möglich, den ganzen E-Mail-Server ungestört auf eine externe Festplatte zu kopieren. Der Datendieb selbst galt als schwieriger Mitarbeiter, der sich gemobbt gefühlt habe, oft krankgeschrieben gewesen sei und in Eigenregie Master-Passwörter geändert habe, damit keiner ausser ihm auf die Datenbank zugreifen könne.

Wie lassen sich die Frauds aber verhindern? «Technische Massnahmen sind nötig, aber immer auch begrenzt, da sie nicht in der Lage sind, den Kontext zu erkennen», erklärt Security-Experte Baumgartner. Grösstes Augenmerk müsse deshalb auf den Faktor Mensch gelegt werden, der die gefährlichste Bedrohung für die Datensicherheit sei. Damit Mitarbeiter aufmerksam bleiben und dem Unternehmen loyal gegenüberstehen, braucht es aber auch eine gewisse Zufriedenheit, weiss Baumgartner: «Wer zufrieden ist, hält die Augen offen und ist bereit, sich mit dem Arbeitgeber zu identifizieren und in seinem Sinne zu handeln.»

INDIKATOREN ERKENNEN

Das IT-Security-Unternehmen Symantec hat sich auf die Suche nach den wichtigsten Indikatoren für Frauds gemacht und in der Studie die häufigsten Gründe für den internen Datenklau zusammengefasst (Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property, 2011): Ganz oben auf der Hitliste stehen demnach Unstimmigkeiten, wem geistiges Eigentum gehört (siehe der Fall Peter K.), viele Überstunden und Streit über Kompensationszahlungen. Auch eine Versetzung oder die nicht genau definierte Rolle eines Mitarbeiters nach einer Fusion können als Motivation dienen. Hinzu kommen Faktoren wie die Nichtberücksichtigung bei einer Beförderung, Konflikte mit Kollegen oder Vorgesetzten und/oder schlechte Führung, unrealistische Zielsetzungen, Ärger in der Familie oder finanzielle Probleme.

12 %
Kundeninformationen*

Seitens des Managements werde gerne einmal übersehen, dass ein Mitarbeiter medizinische oder psychische Probleme habe, ein anormales Sozialverhalten an den Tag lege oder bereits früher gegen Gesetze verstossen habe, so der kritische Tenor der Studie. Anzeichen für potenzielles Betrugsrisiko bieten beispielsweise auch Lebensstil und Schwächen von Personen in Schlüsselpositionen. Das müsse nicht zwangsläufig jemand aus dem Management sein. Auch der Nachtwächter, der nachts allein anwesend und Herr über die Alarmanlagen ist, oder der Buchhalter bekleiden Schlüsselpositionen: «Wenn Ihr Buchhalter Montagmorgen mit dem Ferrari vorfährt, müssen Sie sich fragen, ob seine Schwiegermutter gestorben ist oder ob es sich nicht eventuell um einen Firmenwagen handelt, von dem Sie nichts wissen», scherzte Rolf Schatzmann, Chief Risk & Compliance Officer der Zürcher Renova Management AG, anlässlich der diesjährigen Economic-Crime-Intelligence-Konferenz (ECI) in Wien. Die Experten von Symantec empfehlen, persönliche Prädispositionen für die erwähnten Risikofaktoren bei potenziellen Angestellten bereits vor deren Eintritt ins Unternehmen zu prüfen. Laut Symantec ist der interne Datendieb im Durchschnitt 37 Jahre alt, arbeitet meist in technischen Berufen und hat zwar Vereinbarungen zum Schutz vertraulicher Informationen unterschrieben, beachtet diese jedoch nicht.

Die finanzielle Entlohnung von Verbrechen durch ausländische staatliche Stellen, zum Beispiel durch Deutschland für gestohlene Steuerdaten, erhöht zudem den Anreiz zur Delinquenz und schwächt gleichzeitig das Unrechtsbewusstsein. Teile der Gesellschaft und der Politik halten den Datenklau und den Verkauf an den ausländischen Staat (zur Aufklärung eines anderen Vergehens, hier der Steuerhinterziehung) für gerechtfertigt, weshalb sich Datendiebe als eine Art Robin Hood hochstilisieren können.

WAS TUN IM ERNSTFALL?

Das A und O bei Verdacht auf Betrug, Spionage oder Ähnlichem ist die Strukturierung des Problems, erklärt Oberst a. D. Paul Krüger von der Berner Consulting GmbH den Teilnehmern der Wiener Sicherheitskonferenz. Der ehemalige Leiter der Abteilung Armeeplanung der Schweizer Armee und internationaler Experte für die Entwicklung militärischer Führungs- und Nachrichtenbeschaffungskonzepte empfiehlt, sich zuerst einmal klar darüber zu werden, worum es in der aktuellen Situation geht und in welchem Zeitrahmen gehandelt werden muss. Hier kommt auch der Krisenkommunikation nach aussen eine zentrale Rolle zu (vgl. Beitrag ab S. 36). «Bei den CD-Datenklau-Affären der jüngsten Vergangenheit hat die Problemerfassung definitiv nicht rechtzeitig stattgefunden», ergänzt Dr. Michael Alkalay, CEO vom Neeracher Sicherheitsunternehmen AySEC Services. Ist das Problem klar, müsse in einem nächsten Schritt ein überschaubares Netz von Teilproblemen geschaffen sowie die organisatorische Zuständigkeit, Bedeutung und Dringlichkeit festgelegt werden, meint Krüger. Am besten, man spielt schon einmal durch, was passieren könnte, wenn der Ernstfall eintritt.

MAUER DES SCHWEIGENS

Die Fälle von Datenklau in der Schweiz, die durch die Presse bekannt werden, sind allerdings nur die Spitze des Eisbergs. Der Grossteil, sowohl Vorfälle von aussen, etwa Phishing-Aktivitäten beim Onlinebanking, als auch interne Betrügereien, wird erst gar nicht publik. Computerworld hat verschiedene Unternehmen, darunter die Grossbanken, gefragt, was sie in Sachen Fraud-Protection unternehmen. Allerdings will sich – wenig überraschend – bei diesem heiklen Thema niemand gerne in die Karten schauen lassen, geschweige denn Auskunft über konkrete Fälle im eigenen Unternehmen geben. «Grundsätzlich behandeln wir Themen der Sicherheit und die Details darüber vertraulich», lässt uns Valeria Ancarani, Pressesprecherin der Credit Suisse, wissen, denn, begründet sie, «die Offenlegung von Sicherheitsdispositiven trägt bekanntlich nicht zur Sicherheit bei.»

20 %

Source Code*

Dabei schlampen Finanzinstitute bei der Betrugsprävention und -bekämpfung besonders häufig. Laut einer Untersuchung des Cert Insider Threat Center der renommierten Carnegie Mellon Universität (CMU), auf die auch die Symantec-Studie Bezug nimmt, ist vor allem deren Datensicherung mangelhaft. Viele der auftretenden Betrugsfälle gingen auf schwache Informationssicherheitssysteme zurück, die es Insidern – mehrheitlich Managern – erlaube, ihre Zugriffsrechte in irgendeiner Form zu missbrauchen.

Für die Credit Suisse sei höchste Sicherheit bei der Entwicklung und Anwendung aller Technologien und Endgeräte ein prioritäres Anliegen, erklärt die Pressesprecherin: «Wir setzen alles daran, bestmögliche Datensicherheit zu gewährleisten. Das geschieht durch strikteste Definition von Zugriffsrechten, durch technische Massnahmen, z. B. keine Möglichkeit mehr zur Speicherung von Daten auf externe Datenträger, sowie durch Schulungen und Kontrollen.» Dabei arbeiteten Experten aus den Bereichen IT und Risikomanagement sowie aus der Rechtsabteilung eng zusammen, auch um die Mitarbeitenden für das Thema zu sensibilisieren.

«Die Raiffeisenbank», so der Mediensprecher der Raiffeisen Schweiz Genossenschaft, Franz Würth, gegenüber Computerworld, «blieb bis dato von einem Datendiebstahl verschont.» Es sei allerdings unabdingbar, dass Bankenmitarbeiter zur ordentlichen Erledigung ihrer Tätigkeit Zugriff auf Kundendaten gewährt werde. «Die Vergabe der Zugriffsrechte erfolgt sehr restriktiv und wird regelmässig über- →

* QUELLE: SYMANTEC

«Passen Sie mit technischen Systemen auf, die machen Sie blind»

Rolf Schatzmann, Chief Risk & Compliance Officer, Renova

prüft.» Der Prozess beginne zudem bereits bei der Mitarbeiterrekrutierung: «Es wird bewusst darauf geschaut, dass entsprechend vertrauensvolle Mitarbeiter mit einwandfreiem Leumund eingestellt werden», erklärt Würth. Zudem sei der Personenkreis mit Einsicht auf alle Daten sehr klein. Für die sogenannten Steuer-CDs sind primär Listen mit möglichst vielen Kundendaten interessant. Der Raiffeisen Genossenschaft komme diesbezüglich ihre dezentrale Struktur entgegen: Kundendaten werden in der jeweiligen Bank verwaltet. «Das führt dazu, dass ein Raiffeisen-Kunde angehalten ist, seine Bankgeschäfte primär bei seiner Bank abzuwickeln. Folglich besteht zwischen den Banken kein Zugriff auf die entsprechenden Kundendaten, was deren Sicherheit erheblich erhöht», so Würth.

Zwar hat man auch bei der Basellandschaftlichen Kantonalbank im Rahmen einer systematischen Risikoanalyse die Fraud Protection auf dem Radar. Deren Sprecherin Nadja Widmer bringt aber noch einen anderen, wichtigen Punkt zur Sprache: «Am wirksamsten gegen eine Datenweitergabe durch Mitarbeitende sind eine gute Unternehmenskultur und eine möglichst hohe Mitarbeiterzufriedenheit.»

WIRKUNGSVOLLE PRÄVENTION

Im Grunde genommen ist es jedoch äusserst schwierig, dem Problem Herr zu werden, denn die Handlungsmöglichkeiten sind beschränkt. Wird jemand beim Datendiebstahl erwischt, bleibt dem Arbeitgeber oft nicht viel mehr als Abmahnung, Kündigung und Strafanzeige. Besser ist es, von vornherein mögliche technische oder menschliche Schwachstellen zu beseitigen. Unternehmen müssen ihren Mitarbeitern genau sagen, was die Firma von ihnen erwartet, diese Erwartungen in schriftlichen Policies festhalten und soweit möglich mit technischen Massnahmen unterlegen, meint Christoph Baumgartner. Er empfiehlt, in Vertraulichkeitsvereinbarungen bereits ein Strafmass mit aufzuführen, um potenzielle Datendiebe von vornherein abzuschrecken. «Wer mit hohen Geldstrafen und Schadenersatzforderungen im Falle von Zuwiderhandlungen zu rechnen hat, wird es sich zweimal überlegen, sensible Daten zu entwenden», ist Baumgartner überzeugt. In vielen Vertraulichkeitsvereinbarungen werde zwar detailliert erläutert, was unter vertraulichen Daten zu verstehen sei, aber die Folgen eines Verstosses gegen die Vereinbarung seien eher nebulös formuliert.

Grundsätzlich sollte in einem Arbeitsvertrag so detailliert wie möglich festgehalten sein, was erlaubt ist und was nicht. Denn alles, was nicht explizit verboten ist, gilt juristisch gesehen als geduldet. Unternehmen sollten zudem ein Überwachungsreglement erstellen, in dem die Mitarbeiter darüber informiert werden, dass im Verdachtsfall anonymisiert, pseudonymisiert und im Falle der Erhärtung eines Verdachts auch personalisiert überwacht wird. Allerdings darf dabei das Recht der Mitarbeiter auf Persönlichkeitsschutz nicht verletzt werden. «Das ist manchmal ein Drahtseilakt», weiss Baumgartner. Wird ein potenzieller Täter als Risikofaktor erkannt, kann das Unternehmen ihn zwar bis zu einem gewissen Grad überwachen, mehr aber auch nicht. Einem Mitarbeiter auf den blossen Verdacht hin zu kündigen, wäre ein klassischer Fall einer missbräuchlichen Kündigung.

Von technischer Seite empfehlen sich beispielsweise Zugriffsbeschränkungen. Geregelte Zugriffsrechte sind nach den jüngsten Datendiebstählen besonders in der Finanzbranche ein brisantes Thema. Aber auch durch den steigenden regulatorischen Druck rückt das Identity Access Management (IAM) stärker ins Blickfeld. Einer Umfrage des Analystenhauses KuppingerCole und des Herstellers Beta Systems zufolge besteht jedoch in der Finanzindustrie gerade beim Berechtigungsmanagement von elektronischen Mitarbeiterkonten noch Nachbesserungsbedarf. Wie die Studie zeigt, liegt die Verantwortung für das Identity Access Management immer noch hauptsächlich bei der IT, auch wenn die Entscheidung in jüngster Zeit vermehrt von der Leitungsebene getroffen wird.

TOP-RISIKEN DEFINIEREN

Neben der Regelung von Zugriffsrechten empfehlen sich in technischer Hinsicht neben einer Verschlüsselung und Klassifizierung der Daten auch Monitoring-Systeme mit Alarmierungsfunktion, wobei jede Aktivität aufgezeichnet und zeitnah ausgewertet wird. Spezialisten für IT-Forensik können im Verdachtsfall mit Spezial-Software Festplatten, Handys und E-Mail-Verkehr – selbst mit grossen Datenmengen – analysieren und so für Aufklärung und Beweisführung sorgen.

Zur Bedrohungsabwehr und Sicherheitsregulierung sollten Unternehmen neben klaren Regelwerken und technischen Kontrollsystemen vor allem aber auf das soziale Umfeld im Betrieb achten. Es ist wichtig, ein positives Betriebsklima und materielle Anreize bzw. Lohngerechtigkeit zu schaffen sowie Werte wie Rechtsbewusstsein und Loyalität zu fördern. Denn wer allein auf eine möglichst lückenlose Überwachung setzt, wiegt sich in einer trügerischen

«Wer mit hohen Strafen zu rechnen hat, wird es sich zweimal überlegen»

Christoph Baumgartner, CEO OneConsult

Illusion. «Passen Sie auf mit technischen Systemen zur Überwachung, die machen Sie blind», warnt Rolf Schatzmann, Risk- und Compliance-Chef bei Renova. «Es gibt heute beispielsweise relativ wenige brauchbare elektronische Tools für das Riskmanagement.» Er empfiehlt stattdessen, selbstkritisch die drei realen Top-Risiken fürs eigene Unternehmen herauszukristallisieren. «Nehmen Sie den Querdenker Ihres Unternehmens, insofern Sie ihn nicht schon entlassen haben – denn er ist, auch wenn er stört, der wertvollste Mitarbeiter – und lassen Sie ihn die Risiken definieren.» Manchmal helfen dann schon simple Regeln wie zum Beispiel das Handy am Eingang abzugeben, wie es in Banken, Rechenzentren oder bei Verwaltungsratssitzungen heute gang und gäbe ist. Denn die Mittel zur Strafverfolgung sind begrenzt und sie machen in der Regel an den nationalen Schranken halt. →

FRAUD: **RECHTLICHE RELEVANZ**

Sofern ein Tatbestand nachgewiesen werden kann, sind folgende Gesetze relevant:

→ Unbefugte Datenbeschaffung *(Art. 143 StgB)*

Darunter fallen Tatbestände, bei denen ein Täter, um sich oder einen Dritten zu bereichern, sich selbst oder diesem Dritten elektronisch oder vergleichbar gespeicherte oder übermittelte Daten (auch Software) beschafft, die nicht für ihn bestimmt sind und die gegen diesen Zugriff besonders gesichert wurden. Das Strafmass lautet auf bis zu 5 Jahre Gefängnis oder eine Geldstrafe.

Diese Norm ist jedoch nicht anwendbar, wenn Mitarbeiter Daten entwenden, die nicht elektronisch gespeichert wurden (zum Beispiel Kundendaten in Papierform) oder die nicht speziell gegen diesen Zugriff geschützt wurden. Als genügender Schutz wird beispielsweise ein durch Passwort gesicherter Zugang, Verschlüsselung oder auch die Aufbewahrung eines Laptops in einem verschlossenen Raum betrachtet. Wenn der Täter jedoch lediglich ein arbeitsrechtliches Verbot missachtet, um auf diese Daten zuzugreifen, reicht dies nicht aus. Auf Fälle der sogenannten Datenveruntreuung oder Datenunterschlagung, das heisst, wenn dem Dieb Daten anvertraut wurden oder wenn ihm Daten ohne seinen Willen zugekommen sind, ist dieser Paragraf ebenfalls nicht anwendbar.

→ Unbefugtes Eindringen in ein Datenverarbeitungssystem *(Art. 143a StgB)*

Dieser Artikel umfasst den externen Angriff eines Hackers auf dem Weg einer Datenübertragung in ein Datenverarbeitungssystem. Der Angreifer handelt ohne Bereicherungsabsicht und dringt aus Spass, politischen Gründen und/oder in Schädigungsabsicht unbefugt in ein gesichertes System ein. Das gilt auch für einen Angreifer, der bloss Daten beschädigt oder Computerviren in ein System einführt, um dieses zu beschädigen (Art. 144bis, «Datenbeschädigung»).

Reto Hauser
Der selbstständige Wirtschaftsanwalt bei Hauser Partners ist spezialisiert auf IT-Recht und Wirtschaftskriminalität.
→ www.hauserpartners.ch

→ Datenspionage *(Art. 179novies)*

Darunter fällt das unbefugte Beschaffen von besonders schützenswerten Personendaten aus einer nicht frei zugänglichen Datensammlung. «Nicht frei zugänglich» wird dabei weniger streng gehandhabt als «besonders gesichert» gemäss Art. 143 StGB. 179novies erfasst also z. B. das illegale – auch elektronische – Kopieren von nicht frei zugänglichen Persönlichkeitsprofilen aus einem Personaldossier.

→ Bestimmungen gegen den Geheimnisverrat *(Art. 162 StgB, Art. 47 BankG, Art. 273 StGB)*

Der Mitarbeiter, der elektronisch gespeicherte oder übermittelte Daten entwendet, zu denen er berechtigt oder unberechtigt ungehinderten Zugang hat, kann strafrechtlich oft erst belangt werden, wenn ein weiteres pönalisiertes Verhalten hinzukommt – insbesondere der Geheimnisverrat –, für das Geheimhaltungspflicht aufgrund einer gesetzlichen Vorschrift (Art. 320 ff. StGB, Art. 47 BankG, Art. 35 DSG) oder einer vertraglichen Vorschrift besteht. Dabei hat die arbeitsvertragliche Geheimhaltungspflicht (Art. 321a Abs. 4 OR) eine zentrale Bedeutung. Ein Geheimnis ist jedoch durch einen Mitarbeiter noch nicht verraten, wenn er geheime Daten nur nach Hause nimmt und kein Dritter davon Kenntnis erhält.

Ein Mitarbeiter kann also zum Beispiel «wegen Verrat von Fabrikations- und Geschäftsgeheimnissen» oder «dessen Ausnützen für sich oder einen anderen» aufgrund von Art. 162 StGB bestraft werden.

Der Paragraf zum «wirtschaftlichen Nachrichtendienst» (Art. 273 StGB), der genau wie Art. 162 StGB eine Freiheitsstrafe von bis zu 3 Jahren, aber zusätzlich in schweren Fällen eine Freiheitsstrafe von nicht unter 1 Jahr vorsieht, stellt die Fälle von Verrat schweizerischer Wirtschaftsgeheimnisse zugunsten einer ausländischen amtlichen Stelle oder einer ausländischen privaten Unternehmung oder deren Vertretern und Agenten unter Strafe. Bereicherungsabsicht ist dabei nicht erforderlich. Der Tatbestand traf wohl auf die meisten zuletzt bekannt gewordenen Fälle von Datendiebstahl zulasten eines zur Schweizer Wirtschaft zu zählenden Geheimnisherrn und zugunsten einer ausländischen Steuerbehörde zu.

→ Verbotene Handlungen für einen fremden Staat *(Art. 271 StGB)*

Der Artikel stellt das Handeln ausländischer Behörden (z. B. Steuerbehörden) oder von Personen, die für solche Behörden auf dem Territorium der Schweiz tätig werden (z. B., um Bankdaten erhältlich zu machen) unter Strafandrohung.

→ Erpressung *(Art. 156 StGB)*

Dieser Tatbestand, der mit einer Freiheitsstrafe von bis zu 5 Jahren oder Geldstrafe bestraft wird, kann dann Anwendung finden, wenn der Datendieb den Dateneigentümer, zum Beispiel seinen Arbeitgeber, mit der Drohung der Bekanntmachung oder Weitergabe der Daten nötigt, die Daten zurückzukaufen und damit diesen am Vermögen schädigt und sich selbst oder einen Dritten unrechtmässig bereichert.

→ Veruntreuung *(Art. 138 StGB)*

Dieser Tatbestand ist wohl eher nicht auf Daten anwendbar (in der Lehre umstritten, das Bundesgericht hat die Frage noch nicht entschieden), da Daten weder «Sachen» noch «Vermögenswerte» sind, die man veruntreuen könnte. Das Gleiche gilt für die «Datenunterschlagung» –, womit also für unterschlagene Daten Art. 141 bis StGB nicht anwendbar sein dürfte.

→ Urheberrecht *(URG)*

Sind urheberrechtlich geschützte Werke vom Datendiebstahl betroffen, werden also zum Beispiel Computerprogramme des Arbeitgebers vom Arbeitnehmer kopiert und selbst privat benutzt oder an Dritte weiterveräussert, so greift Art. 67 Urheberrechtsgesetz ein. Die Strafandrohung ist, auf Antrag, bis zu 1 Jahr Freiheitsstrafe oder Geldstrafe.

→ Bundesgesetz über unlauteren Wettbewerb *(UWG)*

Das UWG, das wettbewerbsrelevante Sachverhalte regelt, pönalisiert in seinem Art. 4 lit. c die Anstiftung eines Dritten zum Geheimnisverrat eines Arbeitnehmers oder Beauftragten, in Art. 5 die Verwertung anvertrauter oder unrechtmässig zugänglich gemachter fremder Leistung (wie den Weiterverkauf von Konzepten, Plänen oder sonstiger Arbeitsresultate des Arbeitgebers durch den Arbeitnehmer). UWG Art. 6 stellt die Mitteilung oder Verwertung von ausgekundschafteten oder sonst unrechtmässigen erfahrenen Geschäfts- oder Fabrikationsgeheimnissen unter Strafe.

Der «Datenhehler» ist in der Schweiz nicht als Hehler strafbar (Hehlerei kann nur an Sachen begangen werden). Personen, die zur Datenfreigabe anstiften oder davon profitieren, können entweder als Anstifter oder aufgrund von Art. 5 UWG (unbenutztes Verwenden fremder Leistung) oder infolge Verletzung von Art. 162 Abs. 2 (Ausnutzen des Verrats) oder 4 UWG (Verleitung zum Vertragsbruch und zur Auskundschaftung oder Geheimnisverletzung) belangt werden.

Unter Umständen können auch die nachlässig mit Daten umgehenden Unternehmen rechtlich belangt werden; etwa wenn Daten von Kunden anvertraut wurden und diese wegen fehlender oder technisch unadäquater Datensicherung des Unternehmens preisgegeben werden. ←