Fachhochschule Hagenberg in Oberösterreich: Jährliches Security-Forum zum Thema IT-Sicherheit.

Schutz von Geheimnissen

Beim Security-Forum des Hagenberger Kreises am 11. und 12. April 2019 wurden neben technischen und organisatorischen Fragen der IT-Sicherheit auch solche des Geheimnisschutzes erörtert.

Der Schutz von Daten, insbesondere was deren Sicherheit und die der Informationstechnik betrifft, beruht auf soliden Rechtsgrundlagen wie der Datenschutzgrundverordnung oder dem Datenschutzgesetz. Demgegenüber ist die Informationssicherheit nur in manchen Branchen gesetzlich verankert", stellte der Unternehmensberater Mag. Christoph Riesenfelder *(www.riesenfelder.com)* in seinem Einleitungsvortrag zum *Security-Forum 2019* des *Hagenberger Kreises* in der Fachhochschule Hagenberg in Oberösterreich fest. Sonderrechte in diesem Sinn seien das Patent-, Urheber- oder Geschmacksmusterrecht, doch würden sich gerade in innovationsgetriebenen Umgebungen kaum rechtliche Grundlagen finden. Zudem seien die Budgets für Sicherheitsmaßnahmen aus dem Titel „DSGVO" weitgehend ausgeschöpft.

Rechtsgrundlage des Informationsschutzes ist die im Juni 2016 erlassene Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraglicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (Geheimnisschutz- oder Know-how-Richtlinie).

Ziel dieser Richtlinie ist die Förderung von Forschung und Innnovation, die Abschreckung und Bekämpfung von Industriespionage und Geheimnisverrat sowie die Schaffung rascher und wirksamer Maßnahmen zur Beendigung von rechtswidrigem Erwerb sowie von rechtswidriger Nutzung oder Offenlegung von Geschäftsgeheimnissen.

Die Umsetzung dieser Richtlinie in nationales Recht ist in Österreich durch die UWG-Novelle 2018, BGBl I 2018/109, erfolgt, indem im Wesentlichen der dritte Unterabschnitt „Zivilrechtliche Sonderbestimmungen zum Schutz von Geschäftsgeheimnissen" (§§ 26a bis 26j) in das Bundesgesetz gegen den unlauteren Wettbewerb (UWG) eingefügt wurden. Diese Bestimmungen sind seit 29. Jänner 2019 in Kraft (§ 44 Abs. 11).

Geschäftsgeheimnisse als beschränkt bekanntes Wissen über Know-how und Geschäftsinformationen bestimmen den Markterfolg. Durch Absicherung des Zugangs zu diesem Wissen bleibt der Vorteil erhalten. Nach Offenlegung eines Geschäftsgeheimnisses ist für den rechtmäßigen Inhaber der Zustand, wie er vor dem Geheimnisverlust bestanden hat, nicht mehr wiederherstellbar. Dem Betroffenen bleiben zivilrechtliche Ansprüche auf Unterlassung, Beseitigung und bei Verschulden auf Schadenersatz sowie Einforderung unrechtmäßig erzielter Gewinne.

Die Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses mit dem Vorsatz, es zu verwerten, ei-

FOTO: KURT HICKISCH

nem anderen zur Verwertung zu überlassen oder der Öffentlichkeit preiszugeben, ist nach § 123 StGB mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen. Der Täter ist nur auf Verlangen des Verletzten zu verfolgen. Ein mit bis zu drei Jahren Freiheitsstrafe zu bestrafendes Offizialdelikt stellt es dar, ein derartiges Geheimnis zugunsten des Auslands auszukundschaften (§ 124 StGB).

Nach der Definition des § 26b Abs. 1 UWG ist ein Geschäftsgeheimnis eine Information, die

1. geheim ist, weil sie weder in ihrer Gesamtheit noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen zu tun haben, allgemein bekannt noch ohne weiteres zugänglich ist;
2. von kommerziellem Wert ist, weil sie geheim ist; und
3. Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen durch die Person ist, die die rechtmäßige Verfügungsgewalt über diese Information ausübt.

Die „Angemessenheit" von Schutzmaßnahmen richtet sich nach der Art des Geheimnisses, der Branche, der Organisationsgröße und kann, den Umständen nach, in aktiven oder passiven Maßnahmen bestehen. Daten nach Geheimhaltungsstufen zu klassifizieren, ist eine grundlegende Sicherheitsmaßnahme, doch müssen Geschäftsgeheimnisse nicht ausdrücklich als solche bezeichnet werden. Der Geheimhaltungswille kann sich aus den Umständen ergeben. Auch personenbezogene Daten können Geschäftsgeheimnisse sein. Unter Verweis auf ein Geschäftsgeheimnis kann eine Auskunft nach der DSGVO verweigert werden. Die Maßnahmen

Securityforum 2019: Schwerpunktthema Geheimnisschutz.

müssen vom Schutzberechtigten auch tatsächlich gesetzt werden. Bestehende Sicherheitslücken bei ansonsten funktionierenden Schutzmechanismen lassen nicht den Schluss zu, dass kein Interesse an einer Geheimhaltung bestehe. Beispielsweise wird beim Einspielen von Patches eine gewisse Zeit der Erprobung berücksichtigt werden müssen. Absolute Sicherheit ist kein Erfordernis.

Nachdem auch Art. 32 der DSGVO geeignete technische und organisatorische Maßnahmen vorschreibt, um – hinsichtlich personenbezogener Daten – ein dem Risiko angemessenes Schutzniveau zu erreichen, überschneiden sich weite Bereiche des Daten- und des Informationsschutzes. Data Security- und Information-Security-Management-Systeme (DSMS und ISMS) bauen auf denselben Konzepten auf. Daraus ergeben sich Synergieeffekte, deren Nutzung bei knappen Mitteln zu höherer Effizienz führt. Der Fokus sei laut Riesenfelder vom reinen Schutz personenbezogener Daten hin auf einen allgemeinen Informationsschutz zu richten.

Red Teaming. Thomas Hackner, *Hackner Security Intelligence (www. hackner-security.com)* berichtete über Methoden und Vorgangsweisen, die insbesondere im IT-Bereich von finanziell motivierten Angreifern zum Auskundschaften von Geschäftsgeheimnissen eingesetzt werden, umgekehrt aber auch, um im Auftrag eines Unternehmens Schwachstellen aufzudecken. Um physisch in ein Unternehmen zu gelangen, steht am Anfang das *Scouting* – man sieht sich um und sucht Angriffswege. Bestehen Lücken im Zutrittskontrollsystem, wie leicht lassen sich Sperren überwinden? Kann ein Angreifer im Besucherstrom mitschwimmen, genügt es, sich als Handwerker zu tarnen? Stehen Kopiergeräte und Drucker – deren Festplatten eine Menge an Daten gespeichert haben – unbeaufsichtigt auf den Gängen?

Über die IT geführte Angriffe, etwa solche, die zum CEO-Fraud *(hiezu „Öffentliche Sicherheit" Nr. 5-6/16, S. 6-8)* führen, beginnen zumeist mit Phishing-Mails. Der Angreifer schleust sich in die IT des Unternehmens ein und versucht, zu weiteren Informationen von Zielpersonen zu gelangen, was über Suchmaschinen und soziale Netzwerke so weit verfeinert wird, dass Vertrauen aufgebaut wird und Mitarbeiter des angegriffenen Unternehmens kaum noch Bedenken haben, eigenartig erscheinende finanzielle Transaktionen durchzuführen.

„Man kann noch so vorsichtig sein. Cyber-Incidents passieren, und darauf muss ein Unternehmen vorbereitet sein", sagte DI Gerald Kortschak, *sevian7 IT development GmbH (www.sevian7.com)* und Sprecher der IT-Security-Experts der WKO. Kann wirklich jeder einer Mail widerstehen, bei der durch Anklicken der angefügten Excel-Datei der Urlaubsanspruch überprüft werden kann? Wichtig ist, so Kortschak, ein betriebliches Krisenmanagement für den Ausfall von IT-Systemen einzurichten, um die Folgen eines solchen Vorfalls zu minimieren.

SECURITY FORUM

IT-Sicherheit

Der von Studenten der Fachhochschule Hagenberg, Oberösterreich, gegründete *Hagenberger Kreis zur Förderung der digitalen Sicherheit* veranstaltet alljährlich das *Security-Forum*. Zum 17. Mal hat dieses Forum am 11. und 12. April 2019 in der FH Hagenberg stattgefunden. Die Referate wurden parallel in zwei Panels abgehalten, verbunden durch Vorträge im Audi Max. Im Foyer waren auf IT-Sicherheit spezialisierte Firmen mit Ausstellungsständen vertreten. Ziel des *Hagenberger Kreises* ist die Hebung des IKT-Sicherheitsbewusstseins in der Öffentlichkeit. Der Verein hat 620 Mitglieder.

www.hagenbergerkreis.at
www.securityforum.at

Foto: Kurt Hickisch

Christoph Riesenfelder: „Informationssicherheit nur in manchen Branchen gesetzlich verankert."

Thomas Hackner: „Angriffe über die Informationstechnik beginnen zumeist mit Phishing-Mails."

Lukas Feiler: „Security Researcher begeben sich auf die Suche nach Sicherheitslücken in Programmen."

Security Researcher, die sich, aus welchen Motiven auch immer, auf die Suche nach Sicherheitslücken in Programmen begeben, bewegen sich rechtlich auf dünnem Eis, sagte RA Dr. Lukas Feiler, *Baker McKenzie (www.bakermckenzie.com)*. Jede Software ist urheberrechtlich geschützt, jedes Hochladen eines Programms ist eine Vervielfältigung, die von den Lizenzbedingungen des Herstellers abhängig ist. Die bestimmungsgemäße Nutzung durch den rechtmäßigen Nutzer ist durch § 40d UrhG geregelt. *Reverse Engineering* ist nur zur Herstellung der Interoperabilität erlaubt (§ 40e UrhG), nicht aber zum Aufdecken von Sicherheitslücken. *Code Injection* ist urheberrechtlich insofern zulässig, als die Software nicht verändert wird. Eine solche Veränderung tritt allerdings dann ein, wenn ein *Buffer-Overflow* hervorgerufen und Programmdaten überschrieben werden. Urheberrechtlich zulässig sind *Man-in-the-Middle-Attacks,* weil auch hier die Software nicht verändert, sondern bloß der Programmablauf beobachtet wird. Bei *Spoofing*, dem Vortäuschen einer anderen Identität, wird die Software eines Programms ebenfalls nicht verändert.

Ein nach § 118a StGB strafbarer Zugriff auf ein Computersystem, etwa, um zu Passwörtern zu gelangen, liegt vor, wenn sich jemand durch Überwindung einer spezifischen Sicherheitsvorkehrung in der Absicht Zugang verschafft, sich oder einem anderen Unbefugten Zugang zu schutzwürdigen personenbezogenen Daten zu verschaffen oder einem anderen durch die Verwendung von gespeicherten Daten oder des Computersystems einen Nachteil zuzufügen. Überdies stellt der Versuch, „durch Raten und Eingeben von Passwörtern" in ein Computersystem einzudringen, zivilrechtlich eine Besitzstörung dar (OGH 6 Ob 126/12s).

Fraglich ist, ob eine Sicherheitslücke ein Geschäftsgeheimnis im Sinne der §§ 123f StGB und 26a ff UWG darstellt. Ist sie geheim (immerhin kennt sie nicht einmal der rechtmäßige Nutzer), von kommerziellem Wert und Gegenstand von Geheimhaltungsmaßnahmen? Bejaht man diese Frage, kann Inhaber eines solchen Geschäftsgeheimnisses aber nur der sein, der die Verfügungsgewalt darüber besitzt. Der Erwerb durch einen anderen wäre dann rechtswidrig, sofern nichts anderes vereinbart wurde. Der Researcher hätte sich unbefugten Zugang zu einem Geschäftsgeheimnis verschafft.

Es liegt nahe, die Entdeckung einer Sicherheitslücke in einem Programm zu Geld zu machen und das Wissen zu verkaufen. Derartige Angebote stoßen laut Feiler beim Hersteller nicht unbedingt auf Gegenliebe. Die Reaktionen reichen von einer Annahme des Angebots bis zu Klagsdrohungen. Würde allerdings dem Angebot Nachdruck insofern verliehen, dass bei Nichtannahme etwa mit einer wettbewerbsschädlichen Veröffentlichung gerechnet werden müsste, könnte rasch der Tatbestand der Erpressung (§ 144 StGB) erfüllt sein.

Die Veröffentlichung einer Sicherheitslücke birgt die Gefahr, dass die Lücke von anderen zu strafbaren Handlungen ausgenützt wird. Hält man dies ernsthaft für möglich und findet sich damit ab, wird man zum Beitragstäter zu einer Straftat (§ 12 StGB), es sei denn, es könnte davon ausgegangen werden, dass die Lücke mittlerweile geschlossen wurde („soziale Adäquanz" der Beitragshandlung, OGH 12 Os 21/06i. Die Beitragshandlung muss für ihre sonst uferlose Strafbarkeit dem Beitragstäter objektiv zurechenbar sein).

Vorsicht ist geboten, das Wissen um die Sicherheitslücke an Dritte zu verkaufen. Es könnte der Tatbestand der Geldwäsche (§ 165 StGB) erfüllt werden oder, wenn es sich bei dem Dritten um einen Strohmann eines ausländischen Nachrichtendienstes handeln sollte, der Tatbestand des § 319 StGB (Unterstützung eines fremden militärischen Nachrichtendienstes). Auch Verstöße gegen Handelssanktionen wären denkbar. Es ist von einer aktiven Prüfpflicht des Verkäufers auszugehen.

Im Darkweb Daten über gehackte Unternehmen zu erheben, verstößt nicht gegen Geschäftsgeheimnisse, weil Daten im Darkweb nicht als geheim anzusehen sind. Weiters erstreckt sich der Datenschutz nach der DSGVO nur auf natürliche Personen. Allerdings könnte die leichtfertige, unbewiesene Behauptung, ein Unternehmen sei gehackt worden, zu einer Verurteilung wegen Rufschädigung (§ 1330 Abs. 2 ABGB) führen.

Beim Erheben von Daten über gehackte Accounts wird von einem überwiegenden berechtigten Interesse (Art. 6 Abs. 1 lit. f DSGVO) des für diese Daten Verantwortlichen ausgegangen werden können. Jedoch muss derjenige, der die gehackten Accounts ermittelt hat, dies innerhalb angemessener Frist, längstens jedoch innerhalb eines Monats, der betroffenen Person mitteilen (Art. 14 Abs. 3 DSGVO). Er hat weiters die Sicherheit der personenbezogenen Daten zu gewährleisten (Art. 32 DSGVO). Nach § 7 Abs. 1 DSG dürfen für Forschungszwecke, die keine personenbezogenen Ergebnisse zum Ziel haben, alle personenbezogenen Daten verarbeitet werden, die öffentlich zugänglich sind.

Kurt Hickisch

FOTOS: KURT HICKISCH (2), PRIVAT