Barbara Klett*/Sonja Stirnimann**

Cyber-Crime: Verantwortung und Vorgehen im Ernstfall

In der digitalen und mobilen Welt von heute zählen Datenverlust und Cyber-Angriffe zu den operationellen geschäftskritischen Risiken, die jedes Unternehmen im Auge behalten muss. Cyberkriminelle suchen die schwächste Stelle in einem System, welche oft im Faktor Mensch liegt. Solche Attacken finden gegen Banken wie auch gegen Dienstleistungs- oder Produktionsunternehmen statt. Gerade bei mittelgrossen Unternehmen kann ein Cyber-Angriff schnell existenzbedrohlich werden. Bei Verdacht auf Non-Compliance und wirtschaftskriminelle Handlungen ist daher richtiges Handeln unabdingbar. Der vorliegende Beitrag zeigt präventive Handlungsmöglichkeiten und das richtige Vorgehen im Einzelfall auf. Eine Vorbereitung für solche Fälle wird in der Methode des FraudAidKit™ dargelegt, welche in der Form eines «Notfallkoffers» ein adäquates und praxisnahes Instrument zum Vorgehen im Ernstfall aufzeigt.

Dans le monde numérique et mobile d'aujourd'hui, la perte de données et les cyberattaques comptent parmi les risques opérationnels critiques pour la marche des affaires auxquels chaque entreprise doit rester attentive. Les cybercriminels cherchent le point le plus faible d'un système, qui est souvent le facteur humain. De telles attaques visent aussi bien des banques que des entreprises de services ou de production. Une cyberattaque peut rapidement mettre l'existence même d'une entreprise en péril, particulièrement dans le cas d'une PME. C'est pourquoi une réaction adéquate en cas de soupçon de non-compliance et d'actes de criminalité économique est indispensable. Le présent article expose les possibilités d'actions préventives et la réaction correcte dans un cas concret. Une préparation à ce genre de cas est décrite selon la méthode du FraudAidKitTM, qui constitue un instrument adéquat et pratique, sous forme de «kit de premiers secours» pour agir en cas de crise.

Inhalt

I. Einleitung

Die zunehmende Digitalisierung und Vernetzung der heutigen Zeit führt zu einer Intensivierung von Cyber-Risiken. Hacker stehlen Daten und versuchen damit Geld zu erpressen oder machen die Daten unbrauchbar. Gestohlene Kundendaten werden missbräuchlich verwendet oder Hacker verleiten Betroffene zu ungewollten Vermögensdispositionen.

In jüngster Vergangenheit häufen sich die Meldungen zu Cyber-Attacken, und das Ausmass zieht bereits bedrohliche Konsequenzen nach sich. Es besteht jedoch die Tendenz, das Risiko, selber Betroffener solcher Angriffe zu werden, herunterzuspielen. Dies belegen auch aktuelle Studien, wie die neueste Studie «Report to the Nations on Occupational Fraud and Abuse»[1] der Association of Certified Fraud Examiners (ACFE).

Die Fakten zeigen, dass es jedes Unternehmen, unabhängig von dessen Grösse oder dessen nationaler oder internationaler Ausrichtung, treffen kann. Im Schnitt – so die Studie – büssen die geschädigten Unternehmen

* LL.M, Fachanwalt SAV Haftplicht- und Versicherungsrecht, Partner bei Eversheds-Sutherland AG, Zürich – Barbara.Klett@eversheds-sutherland.ch; <www.eversheds-sutherland.ch>.
** Executive M.B.A Financial Services & Insurance HSG, dipl. Wirtschaftsprüferin, Certified Fraud Examiner, CEO und Gründerin der Structuul AG, Zug – Sonja.Stirnimann@structuul.ch; <www.structuul.ch>.

[1] <http://www.acfe.com/regional-report-europe-west> (besucht am 30. Mai 2017). Diese Studie stellt eine Erweiterung des offiziellen «Report to the Nations on Occupational Fraud and Abuse» aus dem Jahre 2016 (vgl. FN 17) dar.

eine Marge von 5% ein.[2] Viele Anlagen, wie beispielweise Systemkomponenten in Zügen und Notstromaggregate in Krankenhäusern, hängen direkt oder indirekt am Netz. Ein Cyber-Angriff kann lebensbedrohliche Stilllegungen von Systemen oder aber Imageschaden und finanzielle Einbussen verursachen, wenn die betroffenen Unternehmen unvorbereitet sind.

II. Begriffsabgrenzung und erfasste Tatbestände

1. Definition

Es besteht keine einheitlich anerkannte Definition für Cyber-Risiken. Sie lassen sich jedoch wie folgt beschreiben:

> Cyber-Risiken sind operationelle Gefahren, die von Informationen ausgehen, die auf Datenträgern und Netzwerken gespeichert sind. Damit sind sämtliche Informationen, welche nicht physisch vorliegen, also sämtliche elektronisch verfügbaren Daten, dem Risiko von Cyber-Angriffen ausgesetzt.

Die Thematik der Cyber-Risiken gehört im weiteren Sinne zum Oberbegriff «White Collar Crime», welcher aus dem Jahre 1939 stammt und als Summe aller krimineller Handlungen, welche das Unternehmen direkt oder indirekt schädigen und die Regeln des Vertrauens und der Integrität im Wirtschaftsleben missachten, umschrieben werden kann.[3] Darunter fällt ebenfalls der sog. Arbeitgeber-Betrug (occupational fraud), der im Missbrauch der beruflichen Stellung für persönliche Bereicherung durch vorsätzlichen Missbrauch oder Falschverwendung der Ressourcen (Zeit, Geld, Güter, etc.) des Arbeitgebers und/oder der arbeitgebenden Organisation besteht.[4]

2. Risiken

Die Risiken in Zusammenhang mit Cyber-Crime sind von Branche zu Branche unterschiedlich und müssen zwingend unter Einbezug des jeweiligen Geschäftsmodelles sowie der strategischen Ausrichtung, Positionierung und Marktsituation analysiert werden. In der Praxis werden die Risiken rund um das Thema Cyber-Crime oft heruntergespielt, u.a. bei Unternehmen, die nicht primär international tätig sind. Die Tatsache, dass das Risiko von Cyber-Angriffen an den nationalen politischen Grenzen keinen Halt macht, sollte auch mittelständische Unternehmen aufhorchen lassen.

Als nicht abschliessende Auflistung möglicher Risiken können folgende Beispiele genannt werden:

- Angriffe mit dem Ziel des Ausspionierens von Kundendaten oder des Lahmlegens von Systemen z.B. mittels Installation von schädlicher Software (Malware, d.h. Viren, Trojaner);
- Manipulation (Löschung/Veränderung) von Konto- und Finanzdaten bspw. Fälschung von Zahlungsaufträgen oder andere Formen des System-Missbrauchs zur widerrechtlichen Erlangung finanzieller Vorteile;
- Erpressung: Daten-Diebstahl und Androhung von Nachteilen durch Veröffentlichung, Enthüllung dieser Information zwecks Erpressung finanzieller Vorteile;
- Daten- und Wissensverlust durch Entwendung, mögliche anschliessende Vervielfachung und/oder Zerstörung;
- Imageschaden bspw. durch Diebstahl von sensiblen Kunden- und Unternehmensdaten;
- Vermögensdelikte: Veranlassung von Vermögensdispositionen mittels Betrug, Veruntreuung und anderer Delikte.

3. Straftatbestände

Strafrechtlich werden die Delikte in Zusammenhang mit Cyber-Kriminalität unter verschiedene Straftatbestände subsumiert. Dabei sind jeweils folgende Delikte zu prüfen:

- Unrechtmässiges Verschaffen unkörperlicher Daten («Keylogger», «Phishing», Art. 143 Schweizerisches Strafgesetzbuch[5]);[6]
- Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB);[7]

---

[2] <http://www.acfe.com/regional-report-europe-west> (besucht am 30. Mai 2017).

[3] Edwin H. Sutherland, White-Collar Criminality, American Sociological Review (ASR) Vol. 5 No. 1 (1940), 1, definiert «White Collar Crime» als «Sum of all criminal offences which damage an enterprise directly or indirectly and are committed under abuse of the trust and integrity principle ruling in the economic life».

[4] «The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets» (ACFE, Report to the Nations on Occupational Fraud and Abuse, Global Fraud Study, 2016, Introduction, 6, <http://www.acfe.com/rttn-introduction.aspx> [besucht am 7. Juli 2017]).

[5] Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB), SR 311.0.

[6] Art. 143 StGB: Unbefugte Datenbeschaffung.
Abs. 1 Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, sich oder einem andern elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.
Abs. 2 Die unbefugte Datenbeschaffung zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

[7] Art. 143bis StGB: Unbefugtes Eindringen in ein Datenverarbeitungssystem
Abs. 1 Wer auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft;
Abs. 2 Wer Passwörter, Programme oder andere Daten, von denen er weiss oder annehmen muss, dass sie zur Begehung einer strafbaren Handlung gemäss Absatz 1 verwendet werden sollen, in Verkehr bringt oder zugänglich macht, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

– Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB);[8]
– Betrug (Art. 146 StGB);[9]
– Veruntreuung (Art. 138 StGB).[10]

III. Informationen, Empfehlungen und staatliche Massnahmen

Das äusserst dynamische technologische Umfeld und der Mangel an historischen Daten, aus denen Informationen über künftige Schäden extrapoliert werden könnten, sind eine Herausforderung für Behörden, Unternehmer, Versicherungen und sonstige potentielle Betroffene. Wie bei allen Wirtschaftsdelikten sind die Cyber-Betrüger den Ermittlern einen Schritt voraus. Angreifer wenden ausserdem immer komplexere Techniken und manipulative Methoden an.

Cyber-Risiken kennen zudem keine Grenzen, weder zwischen Unternehmen noch geografische oder politische. Auch bei rein innerstaatlichen Transaktionen kann ein Unternehmen aus dem Ausland angegriffen werden, so dass ein grenzüberschreitender Tatbestand entsteht und das Vorgehen danach grenzüberschreitend wird. Der nationale und internationale Informationsaustausch und die Kooperation zwischen privaten und staatlichen Akteuren sind dabei unerlässlich. Diverse private und staatlich geführte Programme befassen sich mit dem Thema. Hier folgt eine Auswahl:

– In der Schweiz wirkt die Melde- und Analysestelle Informationssicherung MELANI. Sie ist für die Prävention von Delikten zuständig. Sie informiert private Computer- und Internetbenutzer sowie kleinere und mittlere Unternehmen (KMU) über Gefahren im Umgang mit modernen Informations- und Kommunikationsmitteln.[11]
– Das Bundesamt für Polizei (fedpol)[12] ist die Anlaufstelle, um strafbare Inhalte und Verhalten im Internet zu melden. Die Meldungen werden nach einer ersten Prüfung und Datensicherung an die zuständigen Strafverfolgungsbehörden im In- und Ausland weitergeleitet. Ausserdem erstellt das fedpol Analysen zur Internetkriminalität und ist zudem der Ansprechpartner für ausländische Stellen.
– Zur Förderung der Kooperation zwischen den Ländern wurde auf europäischer Ebene das Übereinkommen des Europarates vom 23. November 2001 über die Cyberkriminalität am 1. Juli 2004 in Kraft gesetzt. Es ist eine internationale Konvention, die sich mit Computer- und Netzwerkkriminalität befasst. Die Vertragsstaaten werden verpflichtet, ihre Gesetzgebung den Herausforderungen neuer Informationstechnologien anzupassen. Die Schweiz hat das Übereinkommen des Europarates per 1. Januar 2012 in Kraft gesetzt.[13] Das Übereinkommen des Europarates verpflichtet die Vertragsstaaten unter anderem, Computerbetrug, Datendiebstahl, Fälschung von Dokumenten mit Hilfe eines Computers oder das Eindringen in ein geschütztes Computersystem unter Strafe zu stellen. Die Konvention regelt ferner, wie in der Strafuntersuchung Beweise in Form von elektronischen Daten erhoben und gesichert werden. Sie will insbesondere sicherstellen, dass die Untersuchungsbehörden rasch auf elektronisch bearbeitete Daten zugreifen können, damit diese im Laufe des Verfahrens nicht verfälscht oder vernichtet werden. Schliesslich will die Konvention eine schnelle, wirksame und umfassende Zusammenarbeit zwischen den Vertragsstaaten gewährleisten. Ergänzend verabschiedeten das Europäische Parlament und der Rat 2013 die

[8] Art. 147 StGB: Betrügerischer Missbrauch einer Datenverarbeitungsanlage
Abs. 1 Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, durch unrichtige, unvollständige oder unbefugte Verwendung von Daten oder in vergleichbarer Weise auf einen elektronischen oder vergleichbaren Datenverarbeitungs- oder Datenübermittlungsvorgang einwirkt und dadurch eine Vermögensverschiebung zum Schaden eines andern herbeiführt oder eine Vermögensverschiebung unmittelbar darnach verdeckt, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.
Abs. 2 Handelt der Täter gewerbsmässig, so wird er mit Freiheitsstrafe bis zu zehn Jahren oder Geldstrafe nicht unter 90 Tagessätzen bestraft.
Abs. 3 Der betrügerische Missbrauch einer Datenverarbeitungsanlage zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

[9] Art. 146 StGB: Betrug
Abs. 1 Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, jemanden durch Vorspiegelung oder Unterdrückung von Tatsachen arglistig irreführt oder ihn in einem Irrtum arglistig bestärkt und so den Irrenden zu einem Verhalten bestimmt, wodurch dieser sich selbst oder einen andern am Vermögen schädigt, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.
Abs. 2 Handelt der Täter gewerbsmässig, so wird er mit Freiheitsstrafe bis zu zehn Jahren oder Geldstrafe nicht unter 90 Tagessätzen bestraft.
Abs. 3 Der Betrug zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

[10] Art. 138 StGB: Veruntreuung
Abs. 1 Wer sich eine ihm anvertraute fremde bewegliche Sache aneignet, um sich oder einen andern damit unrechtmässig zu bereichern, wer ihm anvertraute Vermögenswerte unrechtmässig in seinem oder eines anderen Nutzen verwendet, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.
Die Veruntreuung zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.
Abs. 2 Wer die Tat als Mitglied einer Behörde, als Beamter, Vormund, Beistand, berufsmässiger Vermögensverwalter oder bei Ausübung eines Berufes, Gewerbes oder Handelsgeschäftes, zu der er durch eine Behörde ermächtigt ist, begeht, wird mit Freiheitsstrafe bis zu zehn Jahren oder Geldstrafe bestraft.

[11] In der Melde- und Analysestelle Informationssicherung MELANI arbeiten Partner zusammen, welche im Umfeld der Sicherheit von Computersystemen und des Internets sowie des Schutzes der schweizerischen kritischen Infrastrukturen tätig sind. Die Website von MELANI (<http://www.melani.admin.ch>) richtet sich an private Computer- und Internetbenutzer sowie an kleinere und mittlere Unternehmen (KMU) der Schweiz.

[12] <http://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/cybercrime.html> (besucht am 30. Mai 2017).

[13] Bundesbeschluss über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18. März 2011, BBl 2010 0527, AS 2011 6293.

Richtlinie über Angriffe auf Informationssysteme,[14] welche das Ziel der Angleichung des Strafrechts der EU-Mitgliedstaaten im Bereich Angriffe auf Daten und Systeme verfolgt. Auf europäischer Ebene beschäftigen sich die zuständigen Organe auch weiterhin eindringlich mit Cyber-Crimes. Bis September 2017 soll beispielsweise die Europäische Cyber-Sicherheitsstrategie überprüft werden, um sie an die neuen EU-weiten Rahmenbedingungen der Cyber-Sicherheit anzugleichen.[15]

– Die EU verfügt über verschiedene Institutionen, welche sich mit Cyber-Kriminalität befassen: 2004 wurde die ENISA (European Network and Information Security Agency) als ein Expertenorgan für die Durchführung spezifischer technischer und wissenschaftlicher Aufgaben errichtet. Ferner beschäftigt sich EUROPOL mit der Cybersicherheit. EUROPOL hat im Januar 2013 das European Cybercrime Centre EC3 errichtet, welches die europäische Kontaktstelle für die Cybersicherheit ist.[16]
– Ferner befassen sich private Unternehmen aus der IT, der Wirtschaft und der Versicherungsbrache mit dem Thema. Private Unternehmen wie auch Berufsverbände haben bereits zahlreiche Untersuchungen vorgenommen.[17]

IV. Beispiele aus der Praxis und Erkenntnisse

Anhand von zwei konkreten Beispielsfällen wird hierfolgt aufgezeigt, dass eine rasche Erkennung und Reaktion auf die allgegenwärtigen Cyber-Risiken unerlässlich sind, damit der Schaden aufgehalten oder wenigstens vermindert werden kann.

Fall 1: Was täglich passieren kann (und passiert)

Am Montagvormittag erhält ein Geschäftsleitungsmitglied von einem Bekannten aus dem geschäftlichen Umfeld eine E-Mail mit der Aufforderung, dem Link in der E-Mail zu folgen, da er seit Neuem mit einer Verschlüsselung E-Mails versendet.

Wie reagieren Sie, wenn:

a) Sie sich gerade letzte Woche ebenfalls informiert haben, wie Sie verschlüsselte (und somit sicherere E-Mails) verschicken können, um dem Empfänger einen höheren Standard an Sicherheit für den Austausch von Informationen zu gewährleisten?
b) Sie mit dem bekannten Geschäftspartner noch vor wenigen Tagen via E-Mail kommuniziert haben und Ihnen dieser erläuterte, dass er nun mit einem neuen IT-Provider unterwegs ist und einen neuen IT-Setup habe, der ihn vollumfänglich zufriedenstellt und der Arbeit entgegenkommt?
c) Dieser Bekannte in einer vertrauenswürdigen Berufsgattung wie z.B. Arzt, Jurist, Treuhänder etc. tätig ist?

Erkenntnisse: Links, welche per E-Mail versendet werden, bergen grundsätzlich ein gewisses Risiko. Ungeachtet des (angeblichen) Absenders ist ihnen stets mit Vorsicht zu begegnen. Oft werden Absender gefälscht oder ein unbedenklicher Link angezeigt, der jedoch auf eine gefälschte Webseite führt. Wie das Beispiel zeigt, darf man sich auch bei angeblich bekannten und vertrauenswürdigen Geschäftspartnern, mit denen man unter Umständen bereits über das in der E-Mail angesprochene Thema der Verschlüsselung gesprochen hat, nicht leichtfertig verleiten lassen, mitgeschickte Links auf vermeintlich bekannte URL-Adressen zu nutzen. Es können auch in diesen Fällen betrügerische Absichten dahinterstehen.

Fall 2: Angriff mit unmittelbarem Verlust

Ihr Unternehmen verkauft eine Produktionsmaschine an Käufer YX. Im Vertrag werden vier Anzahlungen und eine Schlusszahlung nach durchgeführtem Probelauf vereinbart. Die vier Anzahlungen werden in Rechnung gestellt und bezahlt. Ein Hacker mischt sich in der E-Mail-Korrespondenz zwischen Verkäufer und Käufer ein, indem er die «richtigen» E-Mails abfängt und mit einer Fake-E-Mailadresse selber antwortet. Nach erfolgter Lieferung und Probelauf teilt der Hacker dem Käufer mit, dass die fünfte Rate an ein anderes Bankkonto einbezahlt werden soll, da die Firma aufgrund einer Steuerrevision die Geldzuflüsse vom laufenden Jahr aussondern soll, und schickt eine gefälschte Rechnung mit. Der Käufer zahlt die 5. Rate von CHF 450'000 auf das vom Hacker angegebene Konto ein.

Folgende Aktionen sind nach dem Vorfall dringlich angesagt und zu prüfen:

a) Abklärung des Lecks im eigenen IT-System;
b) Kontrolle von allfälligen anderen Manipulationen;
c) Sofortige Beschlagnahme[18] des Bankkontos, an welches die Überweisung erfolgt ist, durch die zuständige Strafbehörde veranlassen;
d) Strafantrag gegen Unbekannt stellen.

Erkenntnisse: Selbst mit einer verbesserten Cyber-Security-Strategie wird es unmöglich sein, Cyber-Risiken vollständig zu beseitigen, dies u.a. weil die Bedrohung durch die immer grössere Abhängigkeit der Unternehmen und der Gesellschaft von digitalen Technologien

[14] Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl. L 218/8 vom 14. August 2013.

[15] <https://ec.europa.eu/digital-single-market/en/cybersecurity> (besucht am 30. Mai 2017).

[16] Hans-Jürgen Lange/Astrid Bötticher, Cyber-Sicherheit, Wiesbaden 2015, 59 ff.

[17] ACFE, Report to the Nations on Occupational Fraud and Abuse, Global Fraud Study, 2016; KPMG, Neues Denken, neues Handeln – Versicherungen im Zeitalter von Digitalisierung und Cyber 2017, Teil B, Cyber; Swiss Re Institute, sigma-Studie 1/2017, Cyber: Bewältigung eines komplexen Risikos.

[18] Strafprozessuale Beschlagnahme ist eine Zwangsmassnahme des Strafprozessrechts, mit welcher die Sicherung von Tatgegenständen oder von Vermögenswerten, die durch eine Straftat erlangt wurden (Konfiskationsbeschlagnahme), erzielt wird. Zu prüfen ist ebenfalls die Möglichkeit einer amtlichen Beschlagnahme von Vermögenswerten des (voraussichtlichen) Schuldners im Hinblick auf eine spätere Zwangsvollstreckung.

anhaltend zunimmt. *Präventiv* müssen Unternehmen ihr Cyber-Risikomanagement sicherstellen (siehe dazu nachfolgend Ziff. V). Nebst *Investitionen in Sicherheitstechnologien* ist ein *verbessertes Bewusstsein* sämtlicher Kader und Mitarbeitenden in Bezug auf aktuelle Methoden der Hacker und andere Cyber-Risiken wirksam. Unternehmen müssen aber insbesondere bereit sein, im Fall der Verwirklichung von Cyber-Risiken *rasch und korrekt zu reagieren* (siehe dazu nachfolgend Ziff. VII).

V. Prävention

Die Prävention von Cyber-Crime setzt ein (Cyber-)Risikomanagement voraus, welches aus verschiedenen Elementen besteht.

a) Compliance umfasst nicht nur die Einhaltung von extern auferlegten Regeln. Im Falle der Prävention geht es – insbesondere im spezifischen Bereich von Wirtschaftskriminalität inkl. Cyber-Crime – darum, zu verstehen, wo die Risiken im Unternehmen liegen. Oft werden aus auf den ersten Blick naheliegenden Gründen sogenannte Risikobeurteilungen halbherzig vorgenommen, in der Annahme, dass bestimmte Risiken das eigene Unternehmen nicht betreffen können. Ebenso unbequem ist die Diskussion über die Risikotoleranz der Verantwortlichen. Was heisst das konkret? Woran wird in einem Unternehmen gemessen, ob die (seitens Verwaltungsrat) vorgegebene Risikotoleranz eingehalten wurde? Das Ziel sollte sein, dass das Management basierend auf der erarbeiteten Risikolandschaft und der Risikotoleranz ein Risikomanagement und eine Strategie entwickelt. Einen Teil dieses Risikomanagements wird durch das regelkonforme Verhalten und dessen Überprüfung wahrgenommen.
b) Aufgrund der Globalisierung, der Ausweitung des Radius und somit der Reichweite der Geschäftstätigkeit sowie international herrschender Regulatorien (um einige Beispiele zu nennen, welche auch für mittelständische Unternehmen schnell zum Risikofaktor werden können: FCPA[19], UK Bribery Act[20], OFAC-Richtlinien[21] etc.)[22] ist die gründliche professionelle Prüfung von Geschäftspartnern (und Mitarbeitenden) vor vertraglicher Bindung in der heutigen Zeit unerlässlich.
c) Vertragliche Absicherungen mit Lieferanten und Dienstleistern. Dabei ist es unerlässlich, die konkreten Bedürfnisse der Vertragsparteien zu untersuchen, um einerseits die Risiken zu erfassen und die Folgen deren Verwirklichung zu regeln und anderseits das erforderliche Gleichgewicht zu finden, damit der Vertrag überhaupt eingegangen werden kann. Darunter sind folgende Aspekte und Elemente zu untersuchen: Haftungsklauseln im Falle von Compliance-Verstössen; Vertragsstrafen in Verbindung mit der Verletzung von vertraglichen Geheimhaltungs- und Datenschutzvereinbarungen, Absicherung der Restrisiken über eine adäquate Versicherungslösung.[23]
d) Absteckung der Risikolandschaft und der Versicherungsdeckung. Auf dem Markt bestehen aktuell mehrere Möglichkeiten von verschieden ausgestalteten Versicherungen. Basierend auf der erstellten Risikolandkarte des jeweiligen Unternehmens gilt es zu beurteilen, welche Art der Versicherung für das Unternehmen und dessen Risikotoleranz der Verantwortlichen zum gegebenen Zeitpunkt die richtige Lösung ist. Eine Versicherung kann nicht alle Risiken abdecken (siehe dazu nachfolgend Ziff. VI), vielmehr haben die Unternehmen präventive Massnahmen innerhalb des Unternehmens mit der Versicherungspolice abzustimmen und zu ergänzen. Dabei gilt es, dem jeweiligen Unternehmen entsprechend Stadium des Lebenszyklus (Start-up, Aufbau, Expansion, Reife, Turnaround, Ablösung, Verkauf), dessen Strategie und dessen Marktumfeld Rechnung zu tragen.

VI. Haftungsrisiken und Versicherbarkeit

In der Schweiz und in anderen europäischen Ländern ist der Versicherungs-Markt in Bezug auf das Cyber-Risiko noch bescheiden. Eine dynamische Entwicklung ist dennoch zu erwarten. Für Versicherungsgesellschaften ist das Cyber-Risiko und somit ein dazu passendes Produkt neu. Es fehlen Erfahrungswerte für ein klares Produktdesign und eine Preisgestaltung. Bisher werden individuelle Einzel- oder Nischenlösungen angeboten.

Mit einer dieser Spezialversicherungen kann sich ein Unternehmen bei Schadenersatzforderungen Dritter absichern. Neben Haftungsszenarien gegenüber Dritten stehen auch eine Fülle möglicher «Eigenschäden» auf der Liste der versicherbaren Risiken. Im Hinblick auf die Versicherbarkeit sind daher Eigenschäden[24] von

[19] Der Foreign Corrupt Practices Act (FCPA) ist ein Antikorruptionsgesetz der USA, das einen weltweiten Anwendungsbereich hat und wodurch sowohl natürliche Personen als auch Unternehmen sanktioniert werden können.

[20] Der UK Bribery Act ist ein britisches Antikorruptionsgesetz, das einen weltweiten Anwendungsbereich hat und wodurch sowohl natürliche Personen als auch Unternehmen sanktioniert werden können.

[21] Das Office of Foreign Assets Control (OFAC) ist eine dem US-amerikanischen Finanzministerium zugeordnete Behörde. Die durch das OFAC verhängten Sanktionen haben gezeigt, dass die US-Behörde auch auf europäische Unternehmen durchgreifen und Bussen anordnen kann.

[22] <https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act>; <http://www.legislation.gov.uk/ukpga/2010/23/contents>; <https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx> (besucht am 30. Mai 2017).

[23] Siehe dazu: Ziff. VI.

[24] Unter Eigenschaden fallen beispielweise Kosten für die Wiederherstellung von Daten und Netzwerken, Ertragsausfallschäden infolge Betriebsunterbrechung, Ausgaben in Verbindung mit Erpressung und Lösegeldforderungen, finanzielle Schäden bei Umleitung von Zahlungs- oder Warenströmen, Kosten durch Veruntreuung

Drittschäden[25], bei welchen ein haftpflichtrechtlicher Anspruch besteht, zu differenzieren.

In Zusammenhang mit der Versicherungsdeckung sind zudem folgende Umstände zu berücksichtigen:

1. Vertraglich übernommene Risiken

Schadenersatzansprüche können auf der Grundlage von «Gesetz» oder «Vertrag» aufgrund der Verletzung von vertraglichen Geheimhaltungs- und Datenschutzvereinbarungen begründet werden. Gängige Policen bieten mitunter lediglich die Absicherung von gesetzlichen Schadensersatzansprüchen und schliessen die vertraglich übernommenen Verpflichtungen ausdrücklich aus. Eine solche Absicherung ist oft unzureichend. Führt eine Datenpanne beispielsweise zu einem Schadenersatzanspruch aus der Verletzung einer Geheimhaltungsvereinbarung oder einem nicht erfüllten Service Level Agreement, ist meist die Absicherung einer «vertraglichen» Haftung erforderlich. Hierzu sind auch verschuldensunabhängige Haftungstatbestände zu berücksichtigen, welche im vertraglichen Bereich meistens keine Versicherungsdeckung geniessen. Im Rahmen des Risiko-Managements sind daher die vertraglich übernommenen Risiken mit der Versicherungsdeckung zu individualisieren und gegenüber zu stellen.

2. Organhaftung für Drittschäden

Die Absteckung der Risikolandschaft und Implementierung eines funktionierenden Sicherheitsmanagements, zu dem selbstverständlich auch die IT-Sicherheit zählt, liegt voll in der Verantwortung der Leitungsorgane.[26] Erleidet ein Unternehmen aufgrund einer Cyberattacke einen wirtschaftlichen Schaden, kann dies zu einer unbeschränkten und persönlichen Haftung des Leitungsorgans mit dem gesamten Privatvermögen führen. Eine entsprechende Deckung (D&O liability) ist daher ebenfalls zu prüfen.

3. Sorgfaltspflichten und Obliegenheiten

Einige Versicherungsprodukte bieten bereits heute auch die Deckung für Betriebsunterbruch, Datenwiederherstellung, Reputation und Krisenmanagement oder Haftpflicht bei Cyber-Risiken an. Dabei hat der Versicherte nachzuweisen, dass er die üblichen und aktuellen Cyber-Schutzsysteme eingesetzt und die für die Branchen erforderlichen Vorsichtsmassnahmen, so auch ein den Bedürfnissen des Unternehmens angepasstes Cyber-Risiko-Management, getroffen hat.[27]

VII. Vorgehen im Ernstfall

Die Unternehmensverantwortlichen sind unter dem Titel Corporate Governance gefordert, das bestehende Krisenmanagement mit Bezug auf die Risiken von Cyber-Angriffen, Non-Compliance und Wirtschaftsdelikten neu zu beurteilen. Die Verantwortung in Bezug auf die bereits mehrmals erwähnten Risiken obliegt dem Verwaltungsrat. Dieser benötigt entsprechend adäquate Entscheidungsgrundlagen.[28]

Anhand eines praktikablen Ansatzes führt die Methode des FraudAidKit™ die Unternehmensverantwortlichen durch die verschiedenen Phasen der Prävention bis zur Vorgehensweise im Ernstfall.

1. Einführung des FraudAidKit™

Cyber-Crime in all seinen Ausprägungen gehört zum Alltag und wird in Zukunft eine grosse Aufmerksamkeit in der Prävention, Aufdeckung und Aufarbeitung (Prevention, Detection Response) von Wirtschaftsdelikten und Non-Compliance darstellen. Unternehmensverantwortliche werden sich vermehrt mit der Thematik auseinandersetzen sowie notwendige präventive und reaktive strategische Führungsinstrumente implementieren müssen, um dem Risiko gerecht zu werden.

Das FraudAidKit™ enthält Elemente, die zur Prävention und zum Krisenmanagement eines Unternehmens gehören. Bei einem gewöhnlichen «Arbeitsunfall» wissen die Betroffenen in jedem Unternehmen und jedem Haushalt, wo die Notfallapotheke steht. Eine Notfallapotheke ermöglicht es den Betroffenen, rasch und adäquat zu handeln. Das FraudAidKit™ verfolgt die gleichen Ziele.

Im Ernstfall oder bei Verdacht auf diesen gilt es zu wissen, wie vorzugehen und wie die erste Phase bis zum Eintreffen der aufgebotenen Spezialisten zu überbrü-

von eigenen Vermögenswerten, finanzielle Schäden bei Diebstahl eigener Immaterialgüter-Rechte (Patente, Urheber-, Marken- und Modellrechte, Geschäftsgeheimnisse etc.), Reputationsschaden des eigenen Unternehmens, interne Kosten von Krisen-Management, Investigations-, Prozess- und Anwaltskosten.

[25] Ansprüche Dritter infolge Verwirklichung von Cyber-Risiken sind beispielsweise Ansprüche aus Datenschutz-Missachtung und aus Persönlichkeits-Verletzung, Ansprüche aus Datenwiederherstellung bei Dritten, Ansprüche aus Diebstahl fremder Immaterialgüter-Rechte (Patente, Urheber-, Marken- und Modellrechte, Geschäftsgeheimnisse etc.), Ansprüche aus Reputationsverlust beim Vertragspartner infolge Fehlverhaltens oder ungenügende Sorgfalt (Pflichtwidrigkeit).

[26] Gemäss Art. 754 Abs. 1 Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (Obligationenrecht, OR), SR 220, sind die Organe «für den Schaden verantwortlich, den sie durch absichtliche oder fahrlässige Verletzung ihrer Pflichten verursachen».

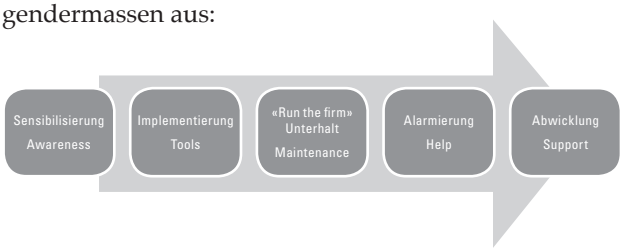
[27] Da ein solcher Nachweis nicht immer einfach zu erbringen ist, empfiehlt es sich, einen Verzicht auf das der Versicherung gemäss Art. 14 Abs. 2 Bundesgesetz über den Versicherungsvertrag vom 2. April 1908 (Versicherungsvertragsgesetz, VVG), SR 221.229.1, zustehende Recht, ihre Leistungen zu kürzen, wenn das Ereignis durch den Versicherten grobfahrlässig herbeigeführt wurde, zu prüfen.

[28] Vgl. FN 26.

cken ist. Dies gewährleistet die Beibehaltung der Handlungsfähigkeit eines Unternehmens.

2. Die Phasen des FraudAidKit™

Die einzelnen Phasen des FraudAidKit™ werden hierfolgt entsprechend erläutert. Ergänzend findet sich am Ende des Artikels eine Checkliste, welche erste Antworten zur Ausgangslage und dem möglichen Bedarf an Werkzeugen und Strukturen liefert. Schematisch dargestellt sieht der Prozess der FraudAidKit™-Methode folgendermassen aus:



Sensibilisierung: Im Rahmen der Sensibilisierung hat sich das Unternehmen u.a. zu fragen: Sind sämtliche Verantwortlichen im Bilde, was alles passieren kann? Wo ist das Unternehmen am verletzlichsten (Risk Exposure and Vulnerability)? Die Sensibilisierung ist der erste Schritt in der Prävention, um die sogenannte «Notfallapotheke» mit den richtigen Werkzeugen und Instrumenten zu befüllen. Je nach Risiko-Landschaft und deren Beurteilung (Risk Assessment) werden unterschiedliche Bestandteile benötigt – diese gilt es unternehmensintern zu identifizieren.

Im Rahmen der Umsetzung der FraudAidKit™-Methode gilt es zu bestimmen, wie die **Werkzeuge** (tools) für die verantwortlichen Entscheidungsträger zugänglich gemacht werden können, um ihre Handlungsfähigkeit zu bewahren, und zwar in jedem der definierten Ernstfälle in seinen Ausprägungen. Die Analysen der definierten Ernstfälle sowie deren Behandlung bei Eintreffen werden basierend auf den verschiedenen relevanten Faktoren der jeweiligen Organisation durchgeführt.

Mit «**Maintenance**» wird der Unterhalt dieser Werkzeuge und Instrumente bezeichnet. Im Ernstfall nützt ein abgelaufenes Medikament nichts, da sich die Betroffenen nicht getrauen, dieses einzunehmen. Genauso verhält es sich mit den implementierten Werkzeugen des FraudAidKit™. Die Organisation wird im Rahmen der Umsetzung der FraudAidKit™-Methode auf Herz und Nieren geprüft. Ziel ist, sicherzustellen, dass im Ernstfall die Organisation richtig reagieren kann. Mit sogenannten «Stress-Tests» werden die implementierten Vorgehensweisen und Massnahmen periodisch überprüft und allfällig vorhandene Schwachstellen aufgezeigt. Schliesslich wollen Betroffene im Ernstfall wissen, wie sie zu reagieren haben, und sich und ihrem Team vertrauen, dass sie reagieren können (und nicht nur wollen).

Der nie erhoffte, doch mehrmals erprobte Ernstfall tritt ein, oft zum ungünstigsten Zeitpunkt. Durch die Implementierung der Methoden und Werkzeuge des FraudAidKit™ wissen Betroffene, wer womit wann und wie zu informieren ist. Dies in Abhängigkeit von den im Voraus evaluierten und definierten Mustern (Fraud Pattern) an möglichen Vorfällen, welche aus dem Risiko-Assessment der Organisation stammen. Dadurch stellen die Verantwortlichen sicher, dass in den ersten Momenten der Erkenntnis wirtschaftskrimineller Handlungen die adäquaten Sofortmassnahmen eingeleitet werden können und verhindern damit, dass zum Beispiel wichtige Beweise durch unprofessionelles Reagieren vernichtet werden.

Im Anschluss erfolgt die **Alarmierung** von definierten Spezialisten (intern und extern, je nach Ausgangslage und Definition durch die Verantwortlichen bei der Erstellung der Checkliste im Rahmen des FraudAidKit™) und die **Aufarbeitung** durch dieses Team an Spezialisten. In dieser Phase ist es für die Organisation existentiell, dass die Experten eng abgestimmt sind und somit effektiv und effizient im Sinne der Problemlösung agieren können. Von Vorteil ist es, wenn sich bereits eingespielte Teams (intern und/oder extern) um den vorliegenden Sachverhalt kümmern und den Verantwortlichen den Rücken insofern freihalten, damit sie sich um das Tagesgeschäft kümmern können und somit ihre Handlungsfähigkeit wahren. In der Praxis hat es sich bewährt, die Untersuchungsteams so klein wie möglich (und so gross wie nötig) zu halten, um eine grösstmögliche Effizienz zu erlangen.

3. Fachkompetenz zur effizienten Umsetzung

In der Praxis hat sich gezeigt, dass erfahrene Experten aus diversen Disziplinen, mit sehr hohem Ermittlungs-, Rechnungslegungs- und Compliance-Verständnis sowie Berichterstattungserfahrung gepaart mit Juristen aus den Sparten Wirtschafts-/Haftpflicht-/Strafrecht und IT-Forensiken eine sehr gute Kombination darstellen. Wenn diese bereits langjährige Erfahrung in gemeinsamer Ermittlungsarbeit nachweisen können, profitieren verantwortliche Führungskräfte von grossen Synergien, welche bei anderen Konstellationen rasch in Summen an Ressourcen enden und zusätzlichen Koordinationsaufwand verursachen. Im Rahmen der dringlichen Sicherungsmassnahmen und der Untersuchungsverfahren hat der Jurist in Zusammenarbeit mit den Sachverhaltsermittlern (inklusive der IT-Forensikern) die Strafbehörde zu unterstützen und, sofern notwendig, zu «schubsen», damit der Sachverhalt mit der erforderlichen Dringlichkeit abgeklärt wird und die Sicherungsmassnahmen prompt und rechtzeitig getroffen werden.

Bei Cyber-Kriminalität ist es unerlässlich, schnell zu handeln. Typische Problematiken in Bezug auf die Strafverfolgung sind auf den Umstand zurückzuführen, dass die Sachverhalte meistens grenzüberschreitend sind. Die Täter üben die Straftaten oft aus dem Ausland aus. Die sofortige Einschaltung der Strafbehörde dient der Beweissicherung und bei Vermögendispositionen der rechtzeitigen Beschlagnahmung oder Sperrung. Hierfür zählt jede Minute. Eine gute Zusammen-

arbeit zwischen dem interdisziplinären Expertenteam mit der Strafbehörde ermöglicht, dass ein Durchsuchungsbefehl mit Beschlagnahme in wenigen Stunden ausgestellt wird.[29] Die Erfahrung zeigt, dass eine konstante fachliche, rechtliche und technische Begleitung im Strafverfahren ebenfalls einer raschen Klärung der Faktenlage und der Verantwortlichkeiten dient. Die Sachverhaltsermittlung, inklusive die ausführliche faktenbasierte Berichterstattung darüber, dient als Grundlage für das Strafverfahren.

4. Schlussfolgerungen

Bei der Absteckung der Risikolandschaft sowie im Rahmen der Umsetzung der FraudAidKit™-Methode spielen das Geschäftsmodell, die Marktsituation und die regulatorischen Rahmenbedingungen der Organisation bzw. des Unternehmens eine wesentliche Rolle. Nicht selten sieht man in der Praxis, dass den Unternehmen das Wissen über die relevanten Cyber-Risiken (Häufigkeit, Schadenspotential) fehlt. Wenn ein Unternehmer beispielsweise als Zulieferer für eine Bank oder ein Krankenhaus agiert, hat dieser spezifische regulatorische Vorschriften einzuhalten und dies sowohl im Rahmen der Organisation als auch im Ernstfall.

Durch strukturiertes Vorgehen können die Risiken erkannt und das Wissen für präventive Massnahmen genutzt werden. Daraus ableitend werden die notwendigen Vorkehrungen – angepasst auf die Risiken der Organisation – getroffen. Die Erarbeitung der Risikolandschaft und Ableitung der Massnahmen stellen die ersten beiden präventiven Schritte in Bezug auf Wirtschaftsdelikte dar. Durch diese Sensibilisierung und das Erlangen der Kenntnis über die möglichen Risiken wird sichergestellt, dass bei Unregelmässigkeiten richtig reagiert werden kann. Studien zufolge werden die meisten Wirtschaftsdelikte über Hinweise, sogenannte «Tips», aufgedeckt. Mit dem Bewusstsein möglicher Risiken steigt die Wahrscheinlichkeit, dass Unregelmässigkeiten entdeckt und somit rapportiert werden.[30]

Die Implementierung eines funktionierenden Sicherheitsmanagements, welches nebst der technischen IT-Sicherheit auch ein Krisenmanagement beinhaltet, liegt vollumfänglich in der Verantwortung der Organe eines Unternehmens. Erleidet ein Unternehmen aufgrund einer Cyberattacke einen wirtschaftlichen Schaden, kann dies zu einer unbeschränkten und persönlichen Haftung des Leitungsorgans mit dem gesamten Privatvermögen führen. Diese Haftung greift bekanntlich bereits bei leichter Fahrlässigkeit und ist demnach ernst zu nehmen (siehe dazu Ziff. V.2).

Die relevanten Risiken zu identifizieren und die notwendigen präventiven Massnahmen in die Wege zu leiten, damit im Ernstfall im Sinne des Unternehmens dessen Handlungs- und Fortführungsfähigkeit gewährleistet werden kann, ist absolut unerlässlich. Unter Einbezug von eingespielten interdisziplinären Teams, welche sich aus internen und externen Experten zusammensetzen, kann innert nützlicher Frist der Prozess der Aufarbeitung des Sachverhalts inklusive der Schadensbegrenzung (zum Nutzen des betroffenen Unternehmens wie auch der Versicherungsdienstleister) effektiv initiiert werden.

Arbeitsinstrumente:

Vorbereitende Checkliste zum FraudAidKit™

1. Sind Notfallszenarien für deliktische Handlungen inklusive Cyber-Angriffe vorhanden?

   _____

2. Sind die Durchlässigkeit und Funktionsfähigkeit der implementierten Notfallszenarien getestet?

   _____

3. Besteht eine (interaktive) Sicherstellung aktuellster Koordinaten innerhalb der implementierten Notfallszenarien? Wenn ja, welche?

   _____

4. Wie ist die interne und externe Kommunikation sichergestellt?

   _____

5. Welches sind die Szenarien, wenn das Management in die deliktischen Handlungen involviert zu sein scheint oder ist?

   _____

[29] Typischer Ablauf einer Strafuntersuchung: Einleitung des Strafverfahrens durch Strafanzeige. Die meisten Delikte sind Offizialdelikte, so dass grundsätzlich keine Strafanzeige erforderlich ist, damit die Strafbehörde tätig wird. In der Praxis zeigt sich aber, dass eine strukturierte und gut begründete Sachverhaltsdarstellung mit Beweismitteln und allenfalls mit Angabe des Schadens der Einleitung und der förderlichen Durchführung der Untersuchung hilft. Die Strafbehörde eröffnet die Untersuchung und klärt den Sachverhalt ab. Dabei kommen folgende Massnahmen in Frage: Verhaftung, Beschlagnahmung, Durchsuchungen, Hausdurchsuchungen, Einvernahmen, Analysen. Bei ausländischer Täterschaft müssen die Massnahmen regelmässig im Rahmen eines Rechtshilfeverfahrens durchgeführt werden. Die Untersuchung der Staatsanwaltschaft wird mittels Einstellung, Strafbefehl oder Anklage abgeschlossen.

[30] Entdeckung von Betrugsfällen: 40,9 % Hinweise, aus ACFE, 2016 Report to the Nations: Western Europe Edition, <http://www.acfe.com/regional-report-europe-west> (besucht am 30. Mai 2017).