Auf der sicheren Seite?

Warum Sicherheit für die Familie und ihr Unternehmen von besonderer Wichtigkeit ist

Von Dr. Jürgen Harrer, Ass.-Prof. Dr. Matthias Waldkirch

ABSTRACT

Viele Familienunternehmen behandeln das Thema Sicherheit stiefmütterlich, was schwerwiegende Auswirkungen auf das Unternehmen und die Unternehmerfamilie haben kann. Aufbauend auf einer aktuellen Studie des Strascheg Institute for Innovation, Transformation & Entrepreneurship (SITE) zeigt der Artikel auf, welchen Risiken Familienunternehmen ausgesetzt sind, warum sicherheitsbezogene Themen immer relevanter werden, gerade Familienunternehmen und Unternehmerfamilien gefährdet sind, und welche Schutzmaßnahmen Familienunternehmen ergreifen. Abschließend geben wir einige Empfehlungen, wie Familienunternehmen das Thema Sicherheit nachhaltig stärken können.

I. Einleitung

Wenn man Familienunternehmen nach zentralen Herausforderungen fragt, denen sie sich in den nächsten Jahren stellen müssen, erhält man ein relativ einheitliches Bild: Es geht um Fragen der Digitalisierung, Innovationskraft, Professionalisierung und besonders des Fachkräftemangels[1]. In einer aktuellen Studie des Strascheg Institute for Innovation, Transformation & Entrepreneurship (SITE) zeigt sich jedoch, dass Familienunternehmen paradoxerweise ein Thema oftmals übersehen – die Sicherheit des Unternehmens und der Familie. Dies ist besonders überraschend, da Familienunternehmer oftmals hohe Anstrengungen unternehmen, um ihr Unternehmen zu erhalten und den Familiennamen zu stärken.[2] Eine fehlende Planung beim Sicherheitsmanagement kann diese Anstrengungen jedoch zunichtemachen.

Anlass für die Studie des SITE war eine Reihe von Schadensereignissen bei Familienunternehmen, über die in den Medien nicht berichtet wurde. Bei der Stiftung Familienunternehmen häuften sich besorgte Anfragen beziehungsweise Bitten um Rat und Unterstützung. Bald erkannte die Stiftung, dass es sich hier nicht um gelegentliche *Schicksalsschläge* handelte, sondern dass sich ein Trend abzuzeichnen scheint: Familienunternehmen und Unternehmerfamilien werden zunehmend mit kriminellen Handlungen konfrontiert und durch sie geschädigt. Das Thema Sicherheit hat für die Familienunternehmen und Unternehmerfamilien in der Vergangenheit offensichtlich an Relevanz gewonnen.

Daher gehen wir im Rahmen dieses Beitrags der Frage nach, welchen Arten von Gefährdungen Familienunternehmen und Unternehmerfamilien aktuell ausgesetzt sind, warum sie möglicherweise besonders gefährdet sind und wie man Unternehmen und Familie angemessen schützen kann.

1 PwC (2018).
2 Deephouse/Jaskiewicz (2013).

INHALT

II. Unternehmens- und Familiensicherheit

Die aktuelle Forschung im Bereich Mittelstand und Familienunternehmen zeigt vielfältige Ansätze, Letztere zu untersuchen und zu verstehen.[3] Familienunternehmen gehen oftmals nur finanziell tragbare Risiken ein, kümmern sich besonders um das Wohl ihrer Mitarbeiter und schreiben Familienkontrolle über das Unternehmen groß.[4] Daher ist es umso verwunderlicher, dass *Sicherheit* in Familienunternehmen nur selten thematisiert wird.

Über viele der erfolgreichen Angriffe auf Unternehmen und Angehörige von Unternehmerfamilien wird in den Medien nicht oder nur wenig berichtet, wodurch der Eindruck entsteht, dass ja eigentlich kaum etwas passiert.

Die Betroffenen kommen hinterher aber zu einer ganz anderen Bewertung der Gefährdungslage, insbesondere bei Fällen wie der Entführung des Unternehmersohns Markus Würth 2015. Doch auch durch Straftaten aus dem Bereich der Wirtschaftskriminalität entstehen große Schäden, wie etwa bei einem vormals aufstrebenden Technologieunternehmen aus Südbayern, bei dem neue Prototypen 2017 durch Drohnen ausspioniert wurden – und das im Markt daher heute keine Bedeutung mehr

3 Nordqvist/Melin/Waldkirch/Kumeto (2015).
4 Gómez-Mejía/Cruz/Berrone/De Castro (2011).

Wichtige Ansatzpunkte und Aufgabenbereiche der Funktion Unternehmenssicherheit

Abb. 1, Quelle: Stiftung Familienunternehmen, 2018

hat. Auch infolge von Erpressung durch Schadsoftware, welche die Firmendaten auf dem Server verschlüsselt (Ransomware), ergeben sich oft große Schäden, wie zum Beispiel bei den Unternehmen Merk und Maersk 2017.

Sicherheit kann zunächst als Phänomen beziehungsweise Zustand verstanden werden, der sich auf einer Skala einstufen lässt. Dabei existiert sie in einer subjektiven und einer objektiven Ausprägung[5]:

Bei der *subjektiven Sicherheit* entwickeln Sicherheitslaien ohne sicherheitsspezifische Ausbildung oder entsprechende Berufserfahrung meist aufgrund einer individuellen Momentaufnahme ein intuitives Bauchgefühl, wobei in der Regel keine stabilen, objektiven Kriterien verwendet werden.

Bei der *objektiven Sicherheit* sammeln und konsolidieren Sicherheitsexperten über einen längeren Zeitraum Informationen aus verschiedenen Quellen (beispielsweise Mitarbeiter, Informanten, Behörden, Dienstleister) und bewerten diese unter Rückgriff auf ihre Ausbildung und jahrelange Berufserfahrung anhand transparenter, spezifischer Kriterien.[6]

Viele Unternehmen haben sich aufgrund von früheren Schadensereignissen für ein professionelles Management der Sicherheitsrisiken entschieden. Dort steht *Unternehmenssicherheit* (*Corporate Security*; *Konzernsicherheit*, *Security*) zusätzlich für eine Unternehmensfunktion, die danach strebt, die Assets eines Unternehmens (Personen, Güter und immaterielle Werte) zu schützen und die geplanten Geschäftsaktivitäten trotz der vorhandenen Sicherheitsrisiken zu ermöglichen.[7]

Dabei kümmert sich die *Security* um die „Abwehr von Gefahren aus regelwidrigem oder kriminellem Handeln und damit aus vorsätzlichem menschlichen Fehlverhalten"[8], während sich die *Safety* beziehungsweise die Arbeitssicherheit als Schwesterdisziplin mit der „Abwehr von Gefahren aus technischem Versagen und fahrlässigem oder versehentlichem menschlichen Fehlverhalten"[9] befasst.

In vielen Unternehmen zeigt sich ein interessantes Phänomen: Besteht eine betriebliche Sicherheitsorganisation, erwartet die Unternehmensleitung häufig, dass diese ihre Arbeit nicht nur erfolgreich und kostengünstig, sondern insbesondere auch *unsichtbar* verrichtet. Dahinter steht das Bestreben, die Mitarbeiter möglichst nicht durch wahrgenommene Schutzmaßnahmen zu verunsichern. Leider verstärkt sich dann jedoch ein meist ohnehin schon unangemessen hohes subjektives Sicherheitsgefühl und führt zu einem geringen Verständnis der Mitarbeiter für die geltenden Sicherheitsbestimmungen und zu einem niedrigen Commitment für neue Schutzmaßnahmen.

Innerhalb der betrieblichen Sicherheitsfunktion „Security" lassen sich Kern- und Stützprozesse unterscheiden.[10] In den Security-Kernprozessen wird die eigentliche Schutzarbeit erbracht; zu ihnen zählen unter anderem Objektschutz, Personenschutz, Reisesicherheit, Informationssicherheit und Supply Chain Security. In den Security-Stützprozessen finden sich die Support-Funktionen und Services, die querschnittlich allen Security-Kernprozessen zur Verfügung gestellt werden; dazu zählen etwa das Security Risk-Management, das Lagezentrum, die internen Ermittlungen und das Security Controlling, mit dem Kosten- und Leistungstransparenz geschaffen werden.[11]

III. Methodisches Vorgehen bei der Studie

Im Rahmen der Studie wurden in einem Zeitraum von acht Monaten 43 Interviews geführt, nämlich mit zehn Familien- »

5 Hummelsheim-Doss (2017).
6 Harrer (2017), S. 41–42; Georgi/Harrer (2019).
7 Dalton (2003), S. 88.
8 Harrer (2017), S. 6.
9 Ebenda.
10 Georgi/Harrer (2019).
11 Harrer (2019).

Frage: „Welchen Gefährdungen sind Unternehmen und Unternehmerfamilien ausgesetzt?“		
Asset-Kategorie	**Beispielhafte Antworten der Unternehmer**	**Beispielhafte Antworten der Sicherheitsexperten**
Personen	Persönliche Risiken für Geschäftsreisende, zum Beispiel Einkäufer in Russland	Belästigung/Stalking; verbale Angriffe/Diffamierung in sozialen Netzwerken;
	Lokale Risiken für Mitarbeiter in Risikoregionen zum Beispiel in Afrika, Mittelamerika oder Südostasien	Körperliche Angriffe; Risiken bei Reisen in unsicheren Regionen
	Erpressung	Entführung und Erpressung; Erpressung zur Korruption; Identitätsdiebstahl und -missbrauch
Güter	Einbruch	Allgemeine Kriminalität (Sachbeschädigung, Einbruch, Diebstahl)
	Diebstahl	Sabotage zur Störung/Unterbrechung der Geschäftsaktivitäten
Immaterielle Werte	Cyberkriminalität	Rufschädigung/Angriff auf das Unternehmensimage
	Unerwünschter Wissenstransfer: Know-how-Träger wechselt zum Wettbewerber	Wirtschaftsspionage (inklusive Lauschangriff; Social Engineering; Cyberattacken)
	Betrug/Geldwäsche; Produkt- und Markenpiraterie (zum Beispiel in China)	

Abb. 2: Beispiele für derzeit wahrgenommene Gefährdungen, Quelle: eigene Darstellung

unternehmern, 15 internen Sicherheitsverantwortlichen, neun externen Sicherheitsberatern sowie neun Vertretern von Versicherungen und Sicherheitsbehörden. Es beteiligten sich hierbei kleine, mittlere und große Unternehmen aus verschiedenen Branchen. Die Interviews wurden schriftlich dokumentiert und stellen die zentrale Grundlage des Berichts und dieses Artikels dar.

Für die fachliche Studienbegleitung etablierte die Stiftung Familienunternehmen einen Expertenbeirat, der sich aus internen Sicherheitsverantwortlichen, externen Sicherheitsberatern und Vertretern von Sicherheitsbehörden zusammensetzte. Nach Abschluss der Datenerhebung im Januar 2018 und der anschließenden Datenauswertung wurde der Studienbericht erstellt.

IV. Ergebnisse

Die Ergebnisse der Studie vermitteln interessante Eindrücke darüber, wie Familienunternehmen mit dem Thema Security umgehen.

1. Gefahren für Familienunternehmen und Unternehmerfamilien

Spricht man Familienunternehmer auf das Thema Security an, dann lautet die spontane Antwort meist sinngemäß: „So etwas wie eine Corporate Security gibt es bei uns nicht. Die brauchen wir auch nicht, denn es ist ja eigentlich noch nie etwas passiert.“

Der letzte Teil dieser Aussage wird dann relativiert, wenn dem Unternehmer auf Nachfragen hin verschiedenste Ereignisse einfallen, wie zum Beispiel Entführungsversuche von Geschäftsreisenden in Mittelamerika, Diebstahl wertvoller Güter in Osteuropa, Schutzgelderpressung in Russland, Wirtschaftsspionage in Deutschland. Offensichtlich gab es in vielen Unternehmen bereits derartige *Security Incidents* beziehungsweise Schadensereignisse, die jedoch kaum als solche wahrgenommen oder zumindest rasch vergessen wurden.

Unsere Studie zeigt, dass die Erkenntnis wächst: Solange es kein funktionierendes Security Incident Reporting gibt, kann niemand Unternehmern realistisch aufzeigen, was schon alles passiert ist – dann erweist sich die subjektiv wahrgenommene Sicherheit im Rückblick als trügerisch.

Ein besonderes Bewusstsein für Gefährdungen durch kriminelle Handlungen, die sich gegen Unternehmer selbst, deren Familien oder das Unternehmen und die eigenen Mitarbeiter richten, konnte nur in wenigen Interviews identifiziert werden. Demgegenüber erkennen die Sicherheitsexperten speziell bei Unternehmen, die sich aufgrund ihrer Technologieführerschaft als Hidden Champions in einer Nische positionieren konnten, erhebliche Gefährdungen durch Wirtschaftsspionage, die über das Internet oder klassisch durch Kopieren, Abhören und Ausfragen praktiziert wird. Darüber hinaus ist jedes Unternehmen, das in bestimmten Regionen geschäftlich tätig ist, einem zum Teil hohen Risiko durch organisierte Kriminalität ausgesetzt.

Die Unternehmer und ihre Familien sind teilweise auch in Deutschland gefährdet, konkret wegen ihrer (regionalen) Bekanntheit, aufgrund ihres Erfolgs, wegen unpopulärer Entscheidungen (etwa Mitarbeiterentlassungen) und wegen des Reichtums, den die Bevölkerung entweder vermutet oder aufgrund von sogenannten Reichenlisten aus den Medien kennt.

2. Steigende Relevanz des Themas Sicherheit

Die Ergebnisse der Studie zeigen weiterhin, dass Schutz und Sicherheit insgesamt an Bedeutung gewonnen haben. Für diese steigende Relevanz bestehen verschiedenste Gründe.[12] Die Zunahme von Geschäftsaktivitäten in risikoreichen Wachstumsregionen im Rahmen der Internationalisierung hat zur Folge, dass Unternehmen in immer größerem Umfang ihre Mitarbeiter und ihr Eigentum erhöhten Sicherheitsrisiken aus-

12 Stiftung Familienunternehmen (2018).

setzen.[13] Das kann der einzelne Geschäftsreisende in Mittelamerika sein, eine Baustelle im Nahen Osten, eine Vertriebsniederlassung in Südostasien oder ein Werk in Nordafrika.[14]
Eine zunehmende Digitalisierung und das leichtfertige Zusammenschalten von sicheren und unsicheren beruflichen sowie privaten Systemen zum Internet of Things ist nicht nur für technologiebegeisterte Mitarbeiter eine Freude, sondern auch für technologieorientierte Kriminelle. Wer bei der Digitalisierung ausschließlich die Chancen im Blick hat und die Risiken verdrängt, der schafft vermeidbare Lücken im Schutzkonzept und gefährdet die Existenz seines Unternehmens.
Nicht nur vor Wahlen und im Sommerloch nimmt die kapitalismuskritische Berichterstattung in den Publikumsmedien zu. Sowohl unbedachte Äußerungen – insbesondere von Politikern und Medienvertretern – als auch bewusste Provokationen wie die Formulierung „obszöner Reichtum“[15] schüren Sozialneid und gesellschaftliche Polarisierung – und liefern im Extremfall sogar die Legitimation für Straftaten.

Die sozialen Medien werden in wachsendem Umfang zur Verbrechensvorbereitung und für Diffamierungskampagnen missbraucht. In kriminellen Kreisen sehr beliebt ist das Ausspähen potenzieller Verbrechensopfer auf Plattformen, auf denen unbedarfte Nutzer regelmäßig und freiwillig detaillierte Informationen über Lebensgewohnheiten, derzeitige Aktivitäten und künftige Vorhaben veröffentlichen.
Weitere Herausforderungen entstehen durch neue Gesetze und regulatorische Bestimmungen wie etwa das Transparenzregister und AnaCredit (Kreditmeldewesen: „Analytical Credit Datasets“). Sicherheitsexperten weisen darauf hin, dass die hier offengelegten Informationen mit vergleichsweise geringem Aufwand von (potenziellen) Tätern mit ideologischem oder kriminellem Hintergrund eingesehen und für die Vorbereitung von Straftaten missbraucht werden können.
Schließlich sind auch verstärkte Aktivitäten staatlicher und privater Akteure im Bereich der Wirtschaftskriminalität festzustellen. Hinsichtlich des hierbei entstandenen Schadens laufen die Einschätzungen weit auseinander, was einerseits an einem uneinheitlichen Security Incident Reporting und andererseits am Fehlen einer Konvention für die Berechnung der wirtschaftlichen Auswirkungen von Schadensereignissen liegt. So schätzte das Bundesamt für Verfassungsschutz den Schaden für das Jahr 2014 „unter Verweis auf Angaben des Bundesverbands der Deutschen Industrie (BDI) auf 50 Mrd. Euro, der Verein Deutscher Ingenieure (VDI) ging von mindestens 100 Mrd. Euro aus“.[16]
Im Fadenkreuz der Angreifer stehen bei der Wirtschaftsspionage und Konkurrenzausspähung in Deutschland verschiedenste Unternehmensbereiche. Häufigstes Ziel ist dabei – wie zu erwarten – der Bereich Forschung und Entwicklung, gefolgt von IT. Überraschenderweise findet sich der Vertrieb auf Platz drei der am häufigsten angegriffenen beziehungsweise ausgespähten Bereiche[17]. Der hierbei stattfindende Informationsabfluss betrifft insbesondere Kalkulationen, Lösungskonzepte, Angebote und Kundendaten.
Wenn hier eine hohe Professionalität der Angreifer – etwa mit intensivem Personalansatz und modernster Technologie – auf ein schwaches Schutzkonzept und ein schmales beziehungsweise stark spezialisiertes Portfolio trifft, dann geht es oftmals nicht nur um schmerzhafte finanzielle Verluste, sondern gar um das Überleben des angegriffenen Unternehmens.
Auf die gestiegene Gefährdung von Bürgern und Unternehmen reagieren auch Institutionen wie das Bundesministerium für Bildung und Forschung, das im Rahmen des Programms „Horizont 2020“ in Teil III auch das Thema „Sichere Gesellschaften – Schutz der Freiheit und Sicherheit Europas und seiner Bürger“ adressiert.[18]

3. Besondere Gefährdung von Familienunternehmen?

Sind inhabergeführte Unternehmen nun stärker gefährdet als kapitalmarktgeführte? In der Tat weisen die Studienergebnisse in diese Richtung.
Das liegt zum einen an einer hohen Personenorientierung auf die Inhaberfamilie, die wie eine Sonne im Zentrum des Systems steht und um die sich das Unternehmen dreht. Wenn die Familie beziehungsweise wichtige Mitglieder ausfallen oder in ihrer Leistungsfähigkeit vermindert werden (etwa durch Schadensereignisse in der Familie), dann leidet in vielen Fällen das ganze Unternehmen darunter. Doch leider sind nicht viele Unternehmer sensibel für mögliche Gefährdungen ihrer Sicherheit, wie folgendes Zitat illustriert:
„Das sehe ich ganz gelassen – wir haben nie ein Problem gehabt – jeder weiß, wo wir wohnen – wir nehmen ganz normal teil am gesellschaftlichen Leben.“
(Quelle: ein Unternehmer im Interview)

Zum anderen sind das Image einer Unternehmerfamilie und die Reputation ihres Familienunternehmens häufig sehr eng miteinander verknüpft. Das führt dazu, dass Diffamierungskampagnen gegen Familienmitglieder leicht zu einem Reputationsschaden für das Familienunternehmen führen können.
Schließlich ist das Familienunternehmen, das sich mit seinen Erfindungen und Patenten als Weltmarktführer in einer Nische positionieren konnte, häufig sehr abhängig von eben diesen immateriellen Werten. Während der Aktienkurs einer breiter aufgestellten DAX-AG den Diebstahl von einigen Patenten besser verkraften kann, bedeutet der Diebstahl von Schlüsseltechnologien und -verfahren für ein Familienunternehmen womöglich das Aus. Eine Verbreiterung des bestehenden Portfolios im Rahmen einer strategischen Neuausrichtung könnte in diesem Fall die Schutzkonzepte für Familie und Unternehmen sinnvoll ergänzen.
Gerade bei Familienunternehmen spielt die ethische Perspektive eine große Rolle, basiert hier doch die erfolgreiche interne Zusammenarbeit üblicherweise auf einem besonderen, wechselseitigen Vertrauensverhältnis zwischen Inhaber und Mitarbeiter. In vielen großen Unternehmen wurden aus solchen »

13 Harrer/Wald (2016).
14 Georgi/Harrer (2018).
15 Fraktion Die Linke (2017).
16 Stiftung Familienunternehmen (2018), S. 60.
17 Corporate Trust (2014).
18 BMBF (2019).

	Zeitliche Perspektive der Schutzmaßnahmen		
	kurzfristig	**mittelfristig**	**langfristig**
Familienunternehmen	• Bestandsaufnahme zur bisherigen Schutzarbeit im eigenen Haus • IT-Grundschutz etablieren • Schlanke Lösung schaffen, zum Beispiel Geschäftsleitungsmitglied als Ansprechpartner; Reporting aller mit Security-Teilaufgaben betrauten Mitarbeiter an die Geschäftsleitung	• Einbindung eines seriösen Sicherheitsberaters für eine objektive Risikoanalyse und ein Schutzkonzept mit Augenmaß • Information und Schulung aller Mitarbeiter • Vernetzung, insbesondere mit Sicherheitsbehörden	• Ganzheitliches Risikomanagement und Business Continuity-Planung für das Unternehmen • sofern möglich: Portfoliodiversifizierung • Krisenszenarien entwickeln und Notfallplanung etablieren • gegebenenfalls eine eigene Sicherheitsorganisation schaffen
Unternehmerfamilie	• Grundsensibilisierung der Familienmitglieder • Grundschutz für IT und Immobilien etablieren	• Einbindung eines seriösen Sicherheitsberaters für eine objektive Risikoanalyse und ein Schutzkonzept mit Augenmaß • Regelmäßige Sensibilisierung der Familienangehörigen: unter anderem Bereitschaft zur kontrollierten Nutzung von sozialen Medien schaffen	• Ganzheitliches Risikomanagement für die Familie • Sensibilisierung für ein konsequent risikobewusstes Verhalten, das heißt eigene Lebensgewohnheiten an die objektiven Sicherheitsrisiken anpassen • gegebenenfalls ein eigenes Family Office etablieren

Abb. 3: Beispielhafte Roadmap für mehr Schutz und Sicherheit, Quelle: eigene Darstellung

nicht-finanziellen Überlegungen heraus bereits umfangreiche Programme aufgelegt, wie die „Zero Harm Culture“ von Siemens, das „Zero Accident Program“ von Beiersdorf oder die „Responsible Care“ von BASF.[19] Die Grundüberlegung hierbei besteht darin, dass die Unternehmen im Kontext von Nachhaltigkeit und Corporate Responsibility Verantwortung für die Abwehr *aller* Gefährdungen zugunsten des Wohls und der Gesundheit ihrer Mitarbeiter am Arbeitsplatz übernehmen.

4. Schutzmaßnahmen für Familienunternehmen

Überraschenderweise ergab sich in einigen Gesprächen die Erkenntnis, dass sich in manchem mittleren oder kleinen Familienunternehmen engagierte Mitarbeiter bereits implizit um Sicherheitsaspekte kümmern. Sie leisten *neben* ihren Hauptaufgaben oftmals wertvolle Schutzarbeit, ohne dass dies den Unternehmern bewusst ist. In solchen Fällen kamen Unternehmer gegen Ende eines Interviews oft zu der erfreuten Feststellung: „Da machen wir ja offensichtlich doch schon einiges im Bereich Security.“

Im *technischen Bereich* sind dies beispielsweise bauliche und technische Maßnahmen wie Zugangskontrollen oder Raumüberwachung (Video; Bewegungsmelder). Im *organisatorischen Bereich* können dies eine Stellvertreterregelung für Schlüsselpersonal, ein Vier-Augen-Prinzip bei finanziellen Transaktionen, unternehmensweite Sicherheitsbestimmungen und Reiserichtlinien oder ein einheitliches Rollen- und Rechtekonzept (*Need-to-know-Prinzip*) sein. Im *personellen Bereich* sind es vorrangig Verhaltensregeln für Führungskräfte und Mitarbeiter, die Vereinbarung von Sicherheitszielen und die Sensibilisierung aller Beschäftigten für Sicherheitsrisiken (zum Beispiel durch „Security Awareness Trainings“).

Abbildung 3 stellt beispielhaft dar, wie mit kurz-, mittel- und langfristiger Perspektive sinnvolle Schutzmaßnahmen zu einem steigenden Sicherheitsniveau führen können. Hierbei sind die kurzfristigen Maßnahmen in vielen Fällen mit eigenen Mitteln beziehungsweise mit den bestehenden Ressourcen zu bewältigen. Die mittel- und langfristigen Maßnahmen erfordern jedoch in der Regel den Rückgriff auf die Expertise externer Ressourcen.

V. Empfehlung und Ausblick

Nicht nur gesetzliche Vorgaben, sondern auch die Erhöhung der Resilienz, die Absicherung der Business Continuity, die Fürsorge für die Mitarbeiter und der Schutz der Unternehmensreputation erfordern ein ganzheitliches Risikomanagement.[20]

„Das Geschäft des Umgangs mit Bedrohungen sollte genauso professionell betrieben werden wie das eigentliche Geschäft!“ (Quelle: ein Unternehmer im Interview)

Hierbei dürfen Sicherheitsrisiken als Teil der operationellen Risiken nicht ignoriert werden; vielmehr muss der Umgang mit ihnen genauso professionell gestaltet werden wie der Umgang mit allen anderen Unternehmensrisiken.

Dazu gehört auch:

- zu akzeptieren, dass Familienunternehmer aufgrund von Erfolg, relativem Wohlstand und internationaler Geschäftstätigkeit höheren Gefährdungen ausgesetzt sind als Mitbürger, die regional als Handwerker, Angestellte oder als Beschäftigte im mittleren öffentlichen Dienst tätig sind, und
- anzuerkennen, dass gute Sicherheitsexperten aufgrund fundierter Ausbildung und jahrzehntelanger Berufserfahrungen in ihrer Arbeit genauso kompetent und glaubwürdig sind wie gute Ärzte, Rechtsanwälte und Wirtschaftsprüfer.

Es geht in diesem Artikel um die Anregung zu einer bewussten, gewissenhaften Beschäftigung mit möglichen Sicherheitsrisiken und ihrer Abwehr. Ziel könnte ein Sicherheitskonzept mit Augenmaß sein, das sich auf eine seriöse, von Experten durchgeführte Risikoanalyse stützt.

19 Harrer (2017), S. 23.

20 Hiles (2011); Romeike/Hager (2013); Trauboth (2016); Välikangas (2010).

Ein seriöser Sicherheitsberater wird keine pauschale, aufgeblähte „Goldrandlösung“ vorschlagen, sondern nach der Risikoanalyse ein individuell angemessenes Schutzkonzept mit dem Unternehmer diskutieren.
Das kann bei vielen Familienunternehmen auch eine schlanke Lösung sein, bei der ein Geschäftsleitungsmitglied als Ansprechpartner für alle Sicherheitsthemen festgelegt wird – denn Sicherheit ist Chefsache. ◆

Literaturverzeichnis

Bundesministerium für Bildung und Forschung (2019):
Sichere Gesellschaften. Schutz der Freiheit und Sicherheit Europas und seiner Bürger. Abgerufen am 31.07.2018 unter https://www.horizont2020.de/einstieg-sicherheit.htm

Corporate Trust (2014):
Industriespionage 2014. Cybergeddon der deutschen Wirtschaft durch NSA & Co.? München.

Dalton, D. R. (2003):
Rethinking Corporate Security in The Post-9/11 Era: Issues and Strategies for Today's Global Business Community. Boston, MA: Butterworth-Heinemann.

Deephouse, D. L./Jaskiewicz, P. (2013):
Do Family Firms Have Better Reputations Than Non-Family Firms? An Integration of Socioemotional Wealth and Social Identity Theories. In: Journal of Management Studies, 50(3), S. 337–360.

Fraktion Die Linke. im Bundestag (2017):
„Obszöner Reichtum wächst – Armut auch“, zuletzt abgerufen am 22.07.2019 unter https://www.linksfraktion.de/themen/nachrichten/detail/obszoener-reichtum-waechst-armut-auch/.

Georgi, C./Harrer, J. (2018):
Projektsicherheit. Internationaler Projekterfolg durch effektive Gefahrenabwehr. In: projektManagement aktuell, 29(5), S. 34–39.

Georgi, C./Harrer, J. (2019):
Das betriebliche Sicherheitsmanagement. Perspektiven der betriebswirtschaftlichen Sicherheitsforschung. In: Wirtschaftsschutz in der Praxis: Positionen zur Unternehmenssicherheit und Kriminalprävention in der Wirtschaft (Sicherheit – Interdisziplinäre Perspektiven). Berlin, Heidelberg: Springer-Verlag (in Druck).

Gómez-Mejía, L. R./Cruz, C./Berrone, P./De Castro, J. O. (2011):
The Bind That Ties. Socioemotional Wealth Preservation in Family Firms. In: The Academy of Management Annals, 5(1), S. 653–707.

Harrer, J./Wald, A. (2016):
Levers of enterprise security control. A study on the use, measurement and value contribution. In: Journal of Management Control, 27(1), S. 7–32.

Harrer, J. (2017):
Security Performance Measurement. Messung und Wertbeitragsermittlung von Leistungen der Unternehmenssicherheit. Herausgegeben von Gleich, R./Wald, A. Münster: LIT Verlag.

Harrer, J. (2019):
Pragmatisches Security Controlling. In: Protector, 47(6), S. 58–59.

Hiles, A. (Hrsg.) (2011):
The Definitive Handbook of Business Continuity Management (3. Aufl.). Hoboken, NJ: Wiley.

Hummelsheim-Doss, D. (2017):
Objektive und subjektive Sicherheit in Deutschland. Eine wissenschaftliche Annäherung an das Sicherheitsgefühl. In: Aus Politik und Zeitgeschichte, 67(32–33), S. 34–39.

Nordqvist, M./Melin, L./Waldkirch, M./ Kumeto, G. (Hrsg.). (2015):
Theoretical Perspectives on Family Businesses. London: Edward Elgar Publishing.

PwC (2018):
Family Business Survey 2018. Der Wert von Werten in der neuen Normalität. https://www.pwc.de/de/mittelstand/pwc-family-business-survey-2018-der-wert-von-werten-in-der-neuen-normalitaet-2018.pdf, zuletzt abgerufen am 22.7.2019.

Romeike, F./Hager, P. (2013):
Erfolgsfaktor Risiko-Management 3.0. Methoden, Beispiele, Checklisten. Praxishandbuch für Industrie und Handel. 3. Auflage. Wiesbaden: Springer.

Stiftung Familienunternehmen (Hrsg.) (2018):
Sicherheit für die Familie und ihr Unternehmen. Analyse von Gefährdungslagen und Schutzmechanismen. Erstellt von der EBS Universität für Wirtschaft und Recht. München: www.familienunternehmen.de

Trauboth, J. H. (Hrsg.) (2016):
Krisenmanagement in Unternehmen und öffentlichen Einrichtungen. Professionelle Prävention und Reaktion bei sicherheitsrelevanten Bedrohungen von innen und außen. Stuttgart: Richard Boorberg.

Välikangas, L. (2010):
The Resilient Organization. How Adaptive Cultures Thrive Even When Strategy Fails. New York, NY: McGraw-Hill.

Dr. Jürgen Harrer ist Forschungsdirektor für Security & Management am Strascheg Institute for Innovation, Transformation & Entrepreneurship (SITE) der EBS Business School. Seine Forschungsinteressen liegen im Bereich Operational Excellence und hier insbesondere im Sales Management sowie im Security Management.

Prof. Dr. Matthias Waldkirch ist Assistenzprofessor für Innovation & Entrepreneurship in Family-Owned Firms am Strascheg Institute for Innovation, Transformation & Entrepreneurship (SITE) der EBS Business School. In seiner Forschung verbindet Matthias Waldkirch Führungs- und Human Relations-Ansätze sowie Corporate Entrepreneurship im Kontext von Familienunternehmen. Seine Forschung beruht dabei hauptsächlich auf qualitativer Methodik.

KEYWORDS
Corporate Responsibility • Risikomanagement • Sicherheit • Wirtschaftskriminalität