Routenplaner Cyber-Security

So stärken Führungsorgane in Produktionsunternehmen die IT-Sicherheit und Cyber-Resilienz

Silvia Weppler, CFO bei der OQ Chemicals Group

Cyber-Kriminalität hat sich mittlerweile durch internationale Organisationen mit arbeitsteiliger Schattenwirtschaft zu einem „hochprofessionellen Business" entwickelt. Attacken auf IT-Systeme und kritische Daten von Unternehmen aller Branchen und Größen, öffentliche Einrichtungen auch mit kritischer Infrastruktur und Staaten steigen weltweit drastisch. Die immer raffinierteren Techniken der Cyber-Kriminellen verändern massiv die Risikolandschaft für Unternehmen und Einrichtungen und führen derzeit jährlich in Deutschland zu Schäden von mehr als 200 Mrd. Euro. Der Gesetzgeber versucht diese zum Schutz von Unternehmen und Organisationen durch Erlass oder Ergänzung von Gesetzen und Richtlinien zu minimieren. Damit sind Vorstand und Aufsichtsrat gesetzlich verpflichtet, geeignete Maßnahmen zu ergreifen und zu überwachen. Sie haften im Schadensfall bei unzureichendem IT-Risiko- und Sicherheitsmanagement. Wie sie dieses Risiko minimieren können, wird nachfolgend detailliert dargestellt.

I. Cyber-Attacken – Risiko für IT-Systeme und Unternehmensdaten

Mit der globalen, flächendeckenden Vernetzung von Datensystemen steigen auch die strategischen und operativen Risiken, sodass Unternehmen und Organisationen die Sicherung nur ihres jeweils eigenen Netzwerkes nicht mehr ausreicht. Denn mit dem Unternehmen vernetzte Stakeholder und Organisationen – wie Kunden, Lieferanten, Systemhäuser, Behörden etc. – können ihrerseits Ziele von Attacken werden und damit auch einen Schwachpunkt für das verbundene Unternehmen darstellen.

Unter sicherheitstechnischen, wirtschaftlichen und politischen Gesichtspunkten gehen die größten Gefahren von Cyber-Angriffen auf die kritische Infrastruktur und sensible Daten von Unternehmen aus.

Fallen IT-Systeme durch Cyber-Angriffe aus und sind Unternehmensdaten nicht mehr abrufbar, kann dies für Unternehmen gravierende Folgen haben. Im schlimmsten Fall kann es zu bestandsgefährdenden Schäden des Unternehmens führen, z.B. durch Verschlüsselung und Diebstahl von Daten zu Störungen bis hin zum Ausfall von Systemen und Produktionsanlagen, aber auch zu Sachschäden. Durch kriminelle Handlungen wie Online-Erpressung, Wirtschaftsspionage, Manipulation an IT-Systemen und Produktionsanlagen drohen hohe finanzielle Einbußen, Umsatzeinbrüche, Verlust von Reputation und Kundenvertrauen, eventuell gefolgt von Schadenersatzklagen von Kunden und Lieferanten.

Daher muss das Unternehmen auf Cyber-Angriffe vorbereitet sein, Cyber-Attacken effektiv begegnen können und regulatorische Anforderungen sowie Geschäftsentwicklungen berücksichtigen. Zielsetzung ist, Angreifer von dem Unternehmensnetzwerk abzuwehren.

II. IT-Sicherheit ist Chefsache!

Die Funktionsfähigkeit der IT-Systeme ist für die Aufrechterhaltung des Geschäftsbetriebs des Unternehmens erforderlich. Damit ist die Cyber-Security geschäftskritisch und überlebenswichtig. Fehlende oder unzureichende Cyber-Sicherheit stellt ein sicherheitstechnisches, juristisches, ökonomisches und organisatorisches Risiko dar, das aufgrund gesetzlicher

INHALT

Keywords
Cyber-Security; IT-Risikomanagement; IT-Sicherheitsmanagement

Normen
§ 91 Abs. 2 AktG, § 43 Abs. 1 GmbHG

Vorschriften und Richtlinien zu bewerten ist.

IT-Sicherheit gehört zu den Kernaufgaben von Vorstand und Geschäftsführung sowie Aufsichtsrat und Beirat. Beide Führungsgremien sind gesetzlich verpflichtet, für ein funktionierendes, präventives IT-Risiko- und Sicherheitsmanagement zu sorgen. Damit haben sie bei der Prävention von Cyber-Attacken eine Schlüsselrolle inne. Sie stehen gemeinsam in der Verantwortung und Haftung. Ihr Engagement ist entscheidend für ein wirksames präventives Cyber-Security-Management. Kurz gesagt: Cyber-Security ist Chefsache!

Dem Vorstand und der Geschäftsführung obliegt die Steuerung des strategischen Unternehmensrisikos. Eine ihrer Kernaufgaben ist die Cyber-Resilienz permanent auszubauen und somit ein umfassendes Cyber-Security-Programm einzurichten und umzusetzen. Darüber hinaus stehen sie in der Pflicht, die umgesetzten Maßnahmen für Cyber-Sicherheit auf ihre Aktualität, Relevanz und Effektivität zu überprüfen.

Somit umfasst der Pflichtenkreis der Geschäftsführung sowohl die Organisations- und Überwachungspflichten zum Schutz der IT-Systeme und Unternehmensdaten im Vorfeld von Cyber-Angriffen, sog. Schadensprävention, als auch die Reaktion auf einen erfolgten Cyber-Angriff. Diese Pflichten obliegen dabei allen Mitgliedern des Vorstands und der Geschäftsführung gemeinsam. Damit trägt die Unternehmensleitung die Gesamtverantwortung auch im Falle einer Übertragung der Zuständigkeit für die IT-Sicherheit an ein bestimmtes Mitglied der Geschäftsleitung, eine Führungskraft oder externe Dienstleister. Eine haftungsrechtlich relevante Übertragung ist dagegen nicht möglich.

Dagegen spielt der Aufsichtsrat eine Schlüsselrolle als Impulsgeber und bei der Überwachung der Management-Aktivitäten hinsichtlich Ressourcen, Budget und Cyber-Security-Maßnahmen. Im Falle von Knowhow-Defiziten in den Bereichen Security Governance und Cyber Risk Management empfiehlt es sich, externe Expertise hinzuziehen.

Die Geschäftsleitung ist nach § 91 Abs. 2 AktG verpflichtet, geeignete Maßnahmen zu treffen, damit Entwicklungen früh erkannt werden, die den Fortbestand der Gesellschaft gefährden. Der Terminus technicus „Bestandsgefährdung" beinhaltet wesentliche Auswirkungen auf die Vermögens-, Ertrags- und Finanzlage des Unternehmens. Hieraus wird die Verpflichtung der Geschäftsleitung abgeleitet, eine „auf Schadensprävention und Risikokontrolle" angelegte Compliance Management-Organisation einzurichten. Gleichartige Vorschriften betreffen auch andere Gesellschaftsformen, beispielsweise in § 43 Abs. 1 GmbHG für den GmbH-Geschäftsführer.

Die Pflichten eines Unternehmens und seiner Organe zur Sicherstellung der IT-Sicherheit und der Unternehmensdaten sind gesetzlich nicht zentral geregelt. Eine rechtliche Verpflichtung zur Sicherstellung von Cyber-Resilienz und Schutz der Unternehmensdaten resultiert aus verschiedenen Gesetzen, Regelwerken und Normen.

Zusammenfassend sind die Führungsorgane gesetzlich verpflichtet, unter Berücksichtigung des Datenschutzes die IT-Sicherheit und den Schutz der Unternehmensdaten in das Risiko-Management- und Compliance-System unternehmensweit zu integrieren. Insgesamt haften alle Führungsorgane persönlich für Schäden durch erfolgreiche Cyber-Angriffe.

III. Umfrageergebnisse des deutschen Mittelstands zur IT-Sicherheit

Nach einer Studie von Deloitte[1] ist ein Großteil des deutschen Mittelstands nur unzureichend gegen IT-Attacken gerüstet – und das, obwohl gerade kleine und mittlere Firmen verstärkt in den Fokus von Cyber-Kriminellen rücken. Cyber-Sicherheit gehört für fast die Hälfte der Befragten bislang nicht zu den Top-Prioritäten der Unternehmensleitung, obwohl Cyber-Angriffe weltweit rasant zunehmen. So können Unternehmen durch Spionage, Online-Erpressung bis hin zur Stilllegung ganzer Geschäftsprozesse großen Schaden erleiden. Vor allem für kleine und mittelständische Unternehmen kann dies existenzbedrohend sein.

Der Branchenverband BITKOM berichtet in diesem Zusammenhang von einem Schaden in Höhe von rund 203 Milliarden Euro, welcher der deutschen Wirtschaft im Jahr 2022 durch Diebstahl sensibler Unternehmensdaten, Spionage, Sabotage und daraus resultierende Betriebsausfälle entstanden ist.[2] Haupttreiber für diese Schäden in Milliarden-Höhe ist vor allem die Zunahme sog. digitaler „Schutzgeld"-Erpressungen.

Dabei ist nahezu jedes Unternehmen betroffen. Es ist lediglich eine Frage der Zeit, wann ein Unternehmen angegriffen wird.

IV. Rechtliche Vorgaben verlangen verschärfte Sicherheitsstandards

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) kommt in seinem Lagebericht vom November 2022[3] zu folgendem Schluss: „Insgesamt spitzte sich im Berichtszeitraum die bereits zuvor angespannte Lage weiter zu. Die Bedrohung im Cyber-Raum ist damit so hoch wie nie." Als Reaktion auf die steigende Bedrohung hat die Europäische Union erstmals Strafmaßnahmen auf Cyber-Angriffe aus Russland und China ver-

1 https://www2.deloitte.com/de/de/pages/mittelstand/contents/studie-mittelstand-und-familienunternehmen-2021.html.

2 https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf.

3 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=8.

hängt. Zudem hat die EU mit einem Rechtsakt zur Cyber-Sicherheit bereits einen einheitlichen EU-weiten Zertifizierungsrahmen eingeführt, da die Cyber-Sicherheit innerhalb Europas auch von internationaler Sicherheit und Stabilität im Cyber-Raum abhängt. Durch die im Amtsblatt L333 der Europäischen Union veröffentlichte NIS-2-Richtlinie kommen auf Betriebe und Einrichtungen mit über 250 Mitarbeitenden und über zehn Millionen Euro Jahresumsatz neue Verpflichtungen für gemeinsame Cyber-Sicherheitsstandards zu. Beispiele sind Audits, Risikoabschätzungen sowie ein zeitnahes Einspielen von Updates und Zertifizierungen. Die Mitgliedstaaten müssen die Richtlinie innerhalb von 21 Monaten nach ihrem Inkrafttreten in nationales Recht umsetzen. In Deutschland trat zudem im Frühjahr 2021 das erweiterte IT-Sicherheitsgesetz 2.0 in Kraft, das Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, sogenannte Betreiber kritischer Infrastrukturen, gesetzlich zur Registrierung und Meldung relevanter IT-Sicherheitsvorfälle bei der Cyber-Sicherheitsbehörde des Bundes (BSI) verpflichtet. „Das IT-Sicherheitsgesetz 3.0" steht bereits in Startlöchern.

V. Zunehmende Professionalisierung der Cyber-Kriminalität

Veraltete IT-Systeme, fehlerhafte Codes, ein leichtfertiger Umgang mit Passwörtern, Manipulationen der Mitarbeitenden durch Social Engineering, mobile Endgeräte aber auch schlecht geschützte Apps erleichtern Cyber-Attacken. Darüber hinaus sind Mitarbeitende in produzierenden Unternehmen oft nur unzureichend im Bereich Cyber-Sicherheit sensibilisiert. In der klassischen IT gibt es außerdem zahlreiche Sicherheitslücken und die vernetzte Operational Technology (OT) ist oft offen wie ein Scheunentor. Die meisten Cyber-Attacken treffen Unternehmen über die Mitarbeitenden, entweder klassisch durch Phishing-E-Mails, über Apps oder mittels Schadsoftware auf USB-Sticks. Cyber-Angriffe werden seit Jahren stetig professioneller und richten sich zunehmend auf unternehmenskritische Prozesse, Infrastruktur und sensible Daten. Sie sind für Angreifer ein sehr lukratives Geschäft, der Ressourcenbedarf ist gering und die Gefahr einer erfolgreichen Strafverfolgung äußerst niedrig.

Die Cyber-Kriminalität hat sich in den vergangenen Jahren ausgehend von Einzelangriffen zu einem hoch „professionellen Business" durch internationale Organisationen mit arbeitsteiliger Schattenwirtschaft im Untergrund entwickelt. Daraus ist ein äußerst lukratives, zukunftsfähiges Geschäftsmodell und ein am stärksten wachsender Markt entstanden.[4]

Die benötigten Fertigkeiten für einen Angriff sind einfach zu erlangen. Cyber-Kriminelle sind dabei durch ihr „training on the job" stets auf dem neuesten Stand. Sie agieren oft international in professionell organisierten Gruppen und können sich dadurch leichter tarnen. Durch den Einsatz von künstlicher Intelligenz (KI) wird es zunehmend auch „Laien" ohne tiefergehende Programmierkenntnisse ermöglicht, Cyber-Angriffe zu initiieren. Im Vergleich hierzu hinkt die Cyber-Risiko-Abwehr in den Unternehmen tendenziell mindestens eine „Generation" hinterher. Kein Unternehmen ist vor einem Angriff gefeit. Auch Großunternehmen und Dax Konzerne sind beliebte, wiederholte Angriffsziele wie die in diesem Jahr bereits bereits mehrfachen Cyber-Angriffe auf den Rüstungs- und Technologiekonzern Rheinmetall am 7.3.2023, 14.4.2023 und 19.5.2023 eindeutig belegen.

Eine Verlagerung von Geschäftsprozessen in die Cloud ist allerdings kein Allheilmittel, obwohl spezifische Technologien entwickelt wurden, um Cloud-Daten und Geschäftsinformationen besser zu schützen. Allerdings variieren die Sicherheitsmaßnahmen je nach Cloud-Anbieter und -Plattform. Besonders der Zugang zu Cloud-Diensten muss geschützt werden. Zusätzlich sollten alle Unternehmensdaten verschlüsselt werden. Wichtig ist es den Standort des Servers zu kennen, da dieser für die den Daten unterliegenden länderspezifischen Rechtsgrundlagen und Gesetzen maßgeblich ist. Besondere Risiken stellen ein Zugang über Smartphones, Zugriff über unsichere Netze und unverschlüsselte Übertragung von Unternehmensdaten und Informationen in die Cloud dar.

Insgesamt tragen sowohl der Cloud-Anbieter als auch das Unternehmen zusammen die Verantwortung für die Sicherheit der Plattform und der Daten.

VI. Handlungsempfehlungen zur Erlangung von Cyber-Resilienz

Cyber-Resilienz basiert auf einer ganzheitlichen Strategie zur Stärkung der Widerstandskraft der IT einer Organisation gegenüber Cyber-Angriffen. „Unternehmen" müssen wissen, wie sie bei potenziellen Cyber-Angriffen reagieren können, um materielle und immaterielle Schäden abzuwenden. Daher sind Präventionsmaßnahmen zu ergreifen und zu überwachen. Der Abschluss einer Cyber-Versicherung kann das Risiko mildern. Allerdings wird für ein Versicherungsangebot üblicherweise die Implementierung eines unternehmensweiten, umfangreichen Sicherungssystems von dem Versicherungsanbieter vorausgesetzt. In diesem Zusammenhang ist zu beachten, dass die Haftung der Organe nur bedingt durch eine Cyber-Versicherung abgemildert werden kann.

Zur Steigerung der Cyber-Resilienz leiten sich die folgenden auf das jeweilige Unternehmen hinsichtlich Branche, Art und Umfang sowie Risikoprofil

4 https://www.srf.ch/audio/trend/organisierte-cyber-kriminalitaet-als-milliardengeschaeft?id=12332524.

individuell abzustimmende wichtige Handlungsempfehlungen ab:

1. Grundsätzlich ist eine ganzheitliche, risikobasierte IT-Sicherheitsstrategie zu erarbeiten und in das unternehmensweite Risiko-Management-System zu integrieren. Ein Cyber-Risiko-Management besteht aus iterativen Prozessen von der Identifikation, über die Quantifizierung und Steuerung bis zur Kontrolle von IT- und Informationssicherheitsrisiken. Da sich die Bedrohungslage permanent verändert, ist eine kontinuierliche Überwachung der eingesetzten IT-Software auf mögliche Verletzbarkeit über den kompletten Lebenszyklus sicherzustellen. Daher sind Sicherheitsprofile so flexibel zu gestalten, dass sie sich problemlos den sich ändernden Bedingungen anpassen lassen.
2. Zur Durchführung von Sicherheitstests sind generell – aber auch aus Haftungsgründen der Organe – spezialisierte IT-Sicherheitsunternehmen zu Rate zu ziehen. Im Rahmen von Penetration-Tests werden Cyber-Angriffe auf die IT-Infrastruktur des Unternehmens simuliert. Zusätzlich können sie eine individuell konfigurierbare Simulationsumgebung zur Verfügung stellen, in der Expert:innen mit einem digitalen Zwilling weitere Industrieszenarien darstellen können. Industrielle Infrastrukturen und ihre Schwachstellen werden auf diese Art und Weise greifbar.
3. Die Ergebnisse dieser Härtetests fließen in ein maßgeschneidertes IT-Sicherheitskonzept und einen detaillierten Maßnahmenplan mit Festlegung von Verantwortlichkeiten ein. Cyber-Security ist niemals eine Standardlösung, sondern immer dynamisch und Ergebnis eines fortlaufenden Prozesses.
4. Zur Minimierung des „menschlichen Faktors" als größtes Risiko für Cyber-Attacken ist die kontinuierliche Sensibilisierung und Zusatzqualifizierung der Mitarbeitenden zur Informationssicherheit durch Schulungen und Workshops ein wichtiges Instrument der IT-Sicherheit. Regelmäßige Erfolgskontrollen und gesteuerte Phishing-Tests sollten das Training ergänzen. Gegebenenfalls sind diese Schulungen auch auf Kunden und Lieferanten mit Zugriff auf das Softwaresystem des Unternehmens auszuweiten.
5. Ein leistungsfähiges Frühwarnsystem zur Erkennung von Auffälligkeiten und zur Abwehr von Cyber-Attacken ist ratsam. Hierzu können ein Security Information and Event Management (SIEM) und Cyber-Security-Software-Analysen eingesetzt werden. Derartige Maßnahmen schaffen Transparenz über die aktuelle IT-Sicherheitslage und den Cyber-Security-Reifegrad eines Unternehmens, dem frühzeitigen Erkennen und Schließen von Schwachstellen, der Entscheidungshilfe zur Optimierung oder Neuausrichtung sowie der Festlegung von Standards. Damit ist es möglich, ein kontinuierliches Monitoring des gesamten Unternehmens-Ökosystems (Unternehmensinfrastruktur, mobile Endgeräte, Third-Party-Anwendungen) zu implementieren, um die Bedrohungslage jederzeit einschätzen und eine effektive Cyberabwehr gewährleisten zu können.
6. Weiterhin ist eine sichere Implementierung von Software-basierten Anwendungen zu gewährleisten. Software-Updates sind unmittelbar nach Erscheinen zu installieren (gemäß der NIS-2-Richtlinie). Im Falle eines Releasewechsels oder beim Einsatz neuer Varianten sind sofortige Updates jeglicher eingesetzten Software vorzunehmen. Dies gilt auch für Maschinen und Produkte beim Kunden vor Ort.
7. Grundsätzlich ist im Vorfeld ein detailliertes Notfallkonzept, ein sog. Plan B, zu entwickeln, um im Falle einer erfolgreichen Cyber-Attacke gewappnet zu sein. Der Fokus liegt auf einem koordinierten Vorgehen zur schnellen Wiederherstellung der IT-Systeme, Datenbanken und Daten durch Backups sowie der sofortigen Trennung mobiler Endgeräte und externer Quellen von der Unternehmensinfrastruktur im Sinne einer primären Schadensbegrenzung. In Abhängigkeit von Art und Umfang des Angriffs sind gegebenenfalls externe Sicherheitsexpert:innen, Forensiker:innen, Polizeibehörden und das BSI (Bundesamt für Sicherheit in der Informationstechnik) einzuschalten. Das BSI bietet auf seiner Homepage diverse Checklisten für KMU bei einem IT-Sicherheitsvorfall an. Existiert eine Cyber-Security-Versicherung, ist das Versicherungsunternehmen entsprechend zu informieren.
8. Im Falle einer Cyber-Attacke müssen die Unternehmensleitung und das Kontrollgremium umgehend informiert werden. Die Unternehmensleitung muss pflichtgemäß reagieren und die Umsetzung des Notfallkonzeptes überprüfen.

   Haftungsrechtlich ist wichtig, dass alle Organisationspflichten zur Einrichtung und laufenden Aktualisierung eines effektiven Cyber-Security-Systems eingehalten wurden und auf den Cyber-Angriff pflichtgemäß reagiert wurde.
9. Besondere Vorsicht sollten Unternehmer:innen und Führungsorgane bei einem Unternehmensverkaufsprozess walten lassen: In dieser Phase werden Unternehmen von Cyber-Kriminellen bevorzugt angegriffen. Häufig werden vor und während des Transaktionsprozesses die notwendigen erhöhten Sicherheits-

anforderungen nicht ausreichend beachtet. Für die Angreifer ergeben sich dadurch lukrative Angriffsziele bei geringerem Ermittlungsrisiko, da sowohl Käufer als auch Verkäufer Interesse daran haben, den Kaufprozess diskret abzuwickeln. Vor Beginn der Due Diligence und damit vor dem Austausch von Unternehmensinformationen ist es daher empfehlenswert eine sog. „Cyber-Due Diligence" durchzuführen, um eventuelle Schwachstellen in den Netzwerken beider Seiten – Käufer und auch Verkäufer – feststellen und beheben zu können.

10. Ein adäquates Budget für alle IT-Sicherheitsmaßnahmen und ausreichend Manpower ist jährlich zu planen und zur Verfügung zu stellen. Cyber-Security ist hierbei als elementare Investition für eine nahezu ungestörte Funktion unternehmenskritischer Prozesse zu werten. Damit wird vor allem finanziellen Schäden bis hin zur Existenzgefährdung des Unternehmens vorgebeugt.

VII. Fazit: IT-Risiko- und Sicherheitsmanagement ist überlebenswichtig

Immer mehr Geschäftsprozesse sind auf eine reibungslos funktionierende IT-Infrastruktur angewiesen. Daher wandelt sich IT-Sicherheit vermehrt zur Unternehmenssicherheit und wird für Firmen und ihre Führungsorgane somit zur haftungsrechtlich nicht delegierbaren Chefsache.

Der Schutz und die Sicherheit des Unternehmens, seiner sensiblen Daten und Informationen muss daher bei jeder Geschäftsentscheidung berücksichtigt werden. Folglich ist die IT-Sicherheit ein elementarer Bestandteil des unternehmensweiten Risiko-Management-Systems.

Bei der Abwehr und Bewältigung von Cyber-Attacken haben Vorstand, Geschäftsführung und Kontrollgremien eine Schlüsselrolle inne, stehen gemeinsam in der Verantwortung und haften im Falle von Versäumnissen persönlich. Digitale Kenntnisse und Erfahrungen sowie Transformationskompetenz spielen mittlerweile bei der Auswahl und Bestellung von Aufsichtsratsmitgliedern und Mitgliedern der Geschäftsführung eine große Rolle. Daher müssen beide Gremien digitale Kompetenzen aufweisen oder sich aneignen und weiter ausbauen. Einhergehend mit den zunehmenden Risiken und gesetzlichen Regularien steigen auch die Anforderungen an den Aufsichtsrat und Beirat. Neben seiner Beratungs- und Überwachungsfunktionen ist er auch Impulsgeber für den Vorstand. Er muss die strategischen Voraussetzungen des Unternehmens, die eigenen Netzwerke sowie das gesamte Geschäftsökosystem des Unternehmens mit Kunden, Lieferanten und anderen Stakeholdern kennen und berücksichtigen.

Es ist damit Aufgabe aller Unternehmen, Einrichtungen und deren Führungsorgane geeignete Präventionsmaßnahmen zu ergreifen, um einerseits gesetzlichen IT-Sicherheitsrichtlinien gerecht zu werden und sich andererseits vor den potenziell verheerenden Folgen von Cyber-Attacken zu schützen. Hierbei gibt es jedoch keinen Status quo, auf dem sie verharren können und der langfristig das nötige Sicherheitsniveau garantiert. Ein Cyber-Security-Management-System ist in der Strategie, der Kultur und den Prozessen eines Unternehmens fest zu verankern. Weiterhin bedarf es flexibler Sicherheitsprofile, die sich dynamisch anpassen lassen. IT-Security-Strategien stehen und fallen mit dem Erfolg ihrer Umsetzung – also der tatsächlichen Operationalisierung. Kurz gesagt: Es gibt heute und künftig keinen hundertprozentigen Schutz vor Cyber-Angriffen.

Cyber-Angriffe werden im Zuge zunehmender globaler Vernetzung voraussichtlich weiterhin drastisch steigen und die Existenz von Unternehmen und Einrichtungen bedrohen. Damit ist die Cyber-Sicherheit zur Vermeidung einer Haftungsfalle und zur Risikominimierung bei der Digitalisierung unabdingbare Voraussetzung.