Cyber Resilience

Ein Leitfaden für Aufsichtsräte zur Widerstandsfähigkeit der Unternehmens-IT

Dr. Edgar Bernardi, Inhaber und COO der avant ag, Agno (Schweiz)

Im Rahmen seiner Beratungs- und Überwachungsfunktion muss ein Aufsichtsrat in der Lage sein zu beurteilen, ob Vorstand und Geschäftsführung in der von ihm zu beaufsichtigenden Organisation ein effizientes Risikomanagement eingeführt haben, das auch die Widerstandsfähigkeit der gesamten IT-Organisation (Cyber Resilienz) sicherstellen kann. Der folgende Beitrag gibt einen Überblick über Anforderungen an die Cyber Resilienz und einen Leitfaden für den Aufsichtsrat als Beurteilungshilfe.

I. Einleitung

Eine der Hauptaufgaben von Aufsichtsräten ist es, den Vorstand auch darin zu überwachen, dass er für wesentliche Risiken, die das zu beaufsichtigende Unternehmen treffen könnten, präventive Maßnahmen definiert und umsetzt bzw. umsetzen lässt *(Enterprise Risk Management)*.

Dieses Unternehmens-Risiko-Management ist ein Teil der *Corporate Resilience*, also der Widerstandsfähigkeit von Unternehmen gegen jede Art von internen und externen dynamischen Veränderungen, insbesondere Risiken, Gefahren oder Bedrohungen (z.B. Energiewende, Korruption, Betrug, Diebstahl, riskante Projekte, Cyber-Angriffe, etc.).

Jedes Unternehmen stützt inzwischen seine Kommunikation, Betriebsabläufe und Bilanzierungen auf ein IT-System bestehend aus IT-Infrastruktur (Netzwerk, Server, Endgeräten, etc.), ERP-Software (Enterprise Ressource Planning) sowie PPS-Software (Produktions- Planung & -Steuerung). Das IT-System ist somit zu einer ganzheitlichen und extrem unternehmenskritischen Ressource geworden, das es präventiv zu schützen gilt vor jeglichem Ausfall, jeder Malfunktionalität oder Manipulation.

IT- und Cyber-Security beinhaltet lediglich den Schutz des IT-Systems, insbesondere vor externen Angriffen. Dieser ist notwendig, aber nicht hinreichend. Entscheidend ist die Widerstandsfähigkeit der gesamten IT-Organisation, auf interne und externe dynamische Veränderungen jeder Art vorbereitet zu sein sowie sich im Ereignisfall schnell anzupassen und reagieren zu können *(Cyber Resilience)*.

Ein Aufsichtsrat, der in der Regel mit neuester IT-Technik im Unternehmen nur bedingt vertraut ist und im Rahmen seiner Governance-Funktion operative Maßnahmen, wenn überhaupt, auch nur begrenzt vorgeben und prüfen kann, tut sich daher naturgemäß schwer, diese Aufgabe umfassend zu bewältigen.

Der folgende Leitfaden soll daher dazu dienen, den Aufsichtsrat bei der Überprüfung zu unterstützen. Anhand des Leitfadens sollte der Aufsichtsrat ohne tiefes technisches IT-Detailwissen in der Lage sein, von Vorstand oder dem IT-Verantwortlichen auf C-Level durch gezielte Fragen und herausforderndes Proben *(challenging)* die Informationen zu erhalten, anhand derer er mittels Plausibilitäten und assoziativer Erfahrung beurteilen kann, wie widerstandsfähig die IT-Organisation und das IT-System des Unternehmens im Allgemeinen und gegen Cyber-Angriffe im Speziellen ist und bleiben wird.

INHALT

Keywords
Cyber Security; Cyber Resilienz; Disruption; Risikomanagement; Überwachungsfunktion

II. Cyber Resilience als Teil der Corporate Resilience

Resilience lässt sich nur schwer treffend ins Deutsche übersetzen. Angelehnt an Naturphänomene, dass ein System stets selbst versucht, sich nach einer Störung oder Deformation relativ rasch wieder in den Urzustand zu bringen – ähnlich einer gebogenen Feder – so lässt sich dies auch auf Unternehmen, Organisationen oder auch IT-Systeme übertragen: *Corporate Resilience* bzw. *Cyber Resilience*.

Es ist also im Falle der *Cyber Resilience* die Fähigkeit der gesamten IT-Organisation, das IT-System des Unternehmens nach einer abrupten Veränderung oder Störung mittels eigener Kräfte, Prozesse und Ressourcen relativ schnell wieder arbeitsfähig

zu machen mit möglichst geringer Beeinträchtigung der Geschäftsprozesse *(business continuity)*. Absicherung *(Cyber Security),* ist sicher eine notwendige, aber keine hinreichende Maßnahme, um *Cyber Resilience* sicherzustellen. Entscheidend sind möglichst für alle Eventualfälle durchdachte Präventivmaßnahmen, die man auf der Basis von umfassender Risikoanalyse *(Cyber Risk Management)* definiert, implementiert und überwacht.

Jedes System ist bekanntlich so schwach wie die schwächste Komponente in einem Gesamtsystem. Jedweder Angriff auf ein solches System richtet sich in der Regel immer auf die schwächste Komponente und irgendein Ausfall des Systems wird in der Regel durch die schwächste Komponente verursacht, da diese wegen der geringeren Belastbarkeit (potenzielle Bruchstelle) mit höherer Wahrscheinlichkeit betroffen ist als andere, stärkere Komponenten. Dies gilt auch und gerade für das IT-System von Unternehmen.

Präventivmaßnahmen als ein Beitrag zur Stärkung der Widerstandsfähigkeit des IT-Systems sind eine wichtige Voraussetzung, solche potenziellen Bruchstellen im System zu reduzieren oder sogar weitgehend zu eliminieren. Permanentes Überwachen und Sicherstellen, dass die Maßnahmen durchgeführt und eingehalten werden, ist ein weiterer Beitrag. Und je besser man auf den Ernstfall vorbereitet ist, die Verantwortlichkeiten definiert und die notwendigen Prozesse festgelegt, geübt bzw. simuliert hat, umso schneller erreicht man wieder einen stabilen Zustand des IT-Systems.

Zunächst ist es daher unerlässlich, den Zustand der Unternehmens-IT und der damit verbundenen Nutzer-, Wartungs- und Überwachungs-Prozesse aktuell zu kennen und permanent zu verfolgen und zu protokollieren, um daraus die Anfälligkeit für Ausfälle oder Angriffe abzuleiten. Der Stress-Test der IT-Organisation und des Systems erfolgt durch eine FMEA genannte Fehler- und Auswirkungs-Analyse (Failure Mode and Effects Analysis), die neben dem theoretischen Durchspielen der verschiedenen Ausfallszenarien auch einen simulierten Hacker-Angriff *(Penetration-Test)* beinhaltet.

Die Ergebnisse aus der FMEA und dem simulieren Hacker-Angriff müssen analysiert und in die Verbesserung der Widerstandsfähigkeit der Unternehmens-IT einfließen. Nur so ist gewährleistet, dass die Widerstandsfähigkeit der IT-Organisation und des IT-Systems permanent gestärkt wird, analog zu einem Qualitäts- Management-System, das in einem Regelkreislauf die Produkt- und Prozess-Qualität permanent verbessert.

Hinzu kommt ein ganz banaler Aspekt, der allerdings vom Autor selbst bei vielen Interims-Projekten und Rechenzentrums-Besichtigungen beobachtet wurde, selbst in namhaften Unternehmen: Gerade im Rechenzentrum *(Serverraum)* und im IT-System kommt es auf Ordnung, Sauberkeit und permanente Pflege und Wartung an, wenn das IT-System stets mit hoher Leistung rund um die Uhr verfügbar sein soll.

IT-Experten und Systemadministratoren neigen nur zu oft dazu, selten oder unvollständig die aktuelle Konfiguration (Hardware, Software) oder Veränderungen daran zu dokumentieren oder zu aktualisieren, Änderungen am IT-System manchmal „on the fly" vorzunehmen, Zugangs- und Alarmsysteme „mal eben zu umgehen, weil es schnell gehen muss", Bedienelemente von Servern nicht ausreichend zu sichern, „Datenschrott" in Form von Altdaten überall aufzubewahren mangels Datensicherung und -bereinigung, etc.

Solche Flüchtigkeiten bzw. Nachlässigkeiten rächen sich dann oft in Form von potenziellen Bruchstellen; die mangelhafte Dokumentation und Datensicherung führt bei Ausfällen und Wiederherstellung dann zu ernsthaften Problemen, weil die vorherige Konfiguration nicht mehr einwandfrei reproduzierbar ist.

Zur ganzheitlichen Beurteilung der Unternehmens-IT, d.h. Zustand, Prozesse, Maßnahmen, Prävention, Risiken, etc., muss der Aufsichtsrat ähnlich einer Unternehmensbewertung *(Due Diligence)* alle Informationen aus Berichten, Fragen, etc. inklusive einer Beurteilung durch Besichtigung initial und dann regelmäßig aggregiert zusammengetragen bekommen, um die *Cyber Resilience* selbst bewerten und feststellen zu können, ob über das Management diese auch sichergestellt wird.

Die Beurteilung, ob ein effizientes System eingeführt und umgesetzt worden ist, lässt sich vom Aufsichtsrat nur in Kenntnis der nötigen Struktur und der gängigen Prinzipien bewältigen, wozu der folgende Leitfaden und die Checkliste eine Hilfestellung geben sollen.

III. Aufgaben des Aufsichtsrats

Generell ist *Cyber Resilience* eine Führungsverantwortung, die nicht an den Systemadministrator des Unternehmens delegiert werden kann, sondern ein IT-Verantwortlicher auf C-Level ist immanent eingebunden und mit den notwendigen Kompetenzen und dem entsprechenden Budget ausgestattet. Wenngleich von jedem einzelnen Mitarbeiter erwartet werden darf, dass er im Rahmen der vorgegebenen Strategie der *Cyber Resilience* mitwirkt, so liegt die Verantwortung für die Widerstandsfähigkeit der Unternehmens-IT in den Händen des obersten Führungskreises des Unternehmens, der das Maß des Risikos zu bewerten sowie die Risiko-Toleranz vorzugeben hat sowie deren Strategie nachhaltig festlegen muss. Sicherheit, Schutz und Abschirmung bedeutet immer auch eine gewisse Einschränkung in der Effizienz der Betriebsabläufe. Insofern kommt der Bewertung der Risiko-Toleranz eine enorme Bedeutung zu, muss mit viel Fingerspitzengefühl angegangen werden und ist ein wesentlicher Bestandteil der Unternehmens-Strategie.

Prinzipien, Werkzeuge, Rahmenstruktur (World Economic Forum)

Der World Economic Report *Advanced Cyber Resilience – Principles and Tools for Boards* definiert drei Bereiche von Board-Prinzipien für *Cyber Resilience*:

I. Prinzipien für *Cyber Resilience*
II. Ordnungsrahmen für Cyber-Risiken
III. Erkennen von Risiken aufkommender Technologien

Prinzipien für Cyber Resilience

Im Folgenden wird ein kurzer Überblick über die Prinzipien und Werkzeuge in Form eines 10-teiligen Werkzeugkastens gegeben, die dann im Leitfaden und der Checkliste konkretisiert werden.

1. Verantwortung für *Cyber Resilience* und Cyber-Risiko: gesamtes Board, primäre Aktivitäten bei existierendem Komitee oder spezielles Cyber Resilience Komitee
2. Kompetenz in *Cyber Resilience* (CR): initiales und regelmäßiges Training und regelmäßige Updates der Board-Mitglieder zu CR-Themen
3. Verantwortlicher auf C-Level für CR, versehen mit ausreichenden Kompetenzen, Board- und internen Zugriffen und Budget
4. Integration von CR und Cyber-Risiko-Bewertung in Geschäftsstrategie, Unternehmens-Risiko-Management sowie Budget- und Ressourcenplanung
5. Risiko-Toleranz: Abgleich Unternehmens-Risiko-Toleranz mit Cyber-Risiko-Toleranz
6. Risiko-Bewertung und Berichtswesen des Managements als Standard-Agenda: quantifizierte und verständliche Bewertung von Cyber-Risiken, Bedrohungen, Ereignisse
7. CR-Plan: Unterstützung des C-Level-Verantwortlichen zur Aufstellung, Implementierung, Test und Verbesserung eines Planes zu *Cyber Resilience*
8. CR-Community: Kollaboration mit anderen Stakeholders suchen und sicherstellen
9. Unabhängige CR-Überprüfung
10. Eigeneffizienz und Leistungsüberwachung des Boards in CR

Ordnungsrahmen für Cyber-Risiken

Der wichtigste und konkrete Teil liegt in der regelmäßigen Überprüfung und Bewertung des Cyber-Risikos auf Basis der Berichterstattung innerhalb des folgenden vorgegebenen Rahmens:

1. Cyber-Risiko-Toleranz in Abgleich mit der Unternehmens-Strategie und der Gesamt-Risiko-Toleranz
2. Cyber-Risiko-Identifikation, gefolgt von Management-Aktionen
3. Festlegung der Risiko-Management-Aktionen
   a. Entschärfung des Risikos (technisch, administrativ, organisatorisch, etc.)
   b. Verlagerung (Versicherung, etc.)
   c. bewusstes Einkalkulieren und Akzeptieren kleinerer oder einschätzbarer Risiken
   d. präventives Vermeiden, wenn Risikopotenztial erkennbar
4. Restrisiko-Bewertung

Die Abbildung 1 gibt eine Übersicht zu Cyber-Risiken.

Folgende allgemeine Ordnungsrahmen für Risiken, insbesondere Cyber-Risiken, teilweise in Form von Standards, sind inzwischen verbreitet (Auswahl):

- *ISO/IEC 27k*: de facto Standard für Risiko-Ordnungsrahmen
- *COBIT* (Control Objectives for Information and Related Technologies, ISACA: Information Systems Audit Control Association): umfassender Ordnungsrahmen für IT-Risiken, inkl. Governance
- *NIST Special Publication (SP) 800* Series: US Standard Cyber Risk-Ordnungsrahmen
- *FIPS* (Federal Information Processing Standards, NIST: National Institute of Standards and Technology)
- *OCTAVE Allegro: Cyber Risk and Resilience Management* (SEI: Software Engineering Institute): Ergänzung zu anderen Ordnungsrahmen
- *PCISSC* (Payment Card Industry Security Standards Council): Überblick
- *Framework for Improving Critical Infrastructure Cybersecurity* (NIST): Überblick
- *Inventory of Risk Management/ Risk Assessment Tools* (ENISA: Europäische Agentur für Netz- und Informationssicherheit): Überblick

Erkennen von Risiken aufkommender Technologien

Neue unternehmerische Vorhaben *(ventures)* sind oft Gegenstand der Diskussion und Entscheidung in Aufsichtsratssitzungen. Dabei werden Chancen, Marktpotenzial, Umsatzerwartungen, etc. ausführlich disku-

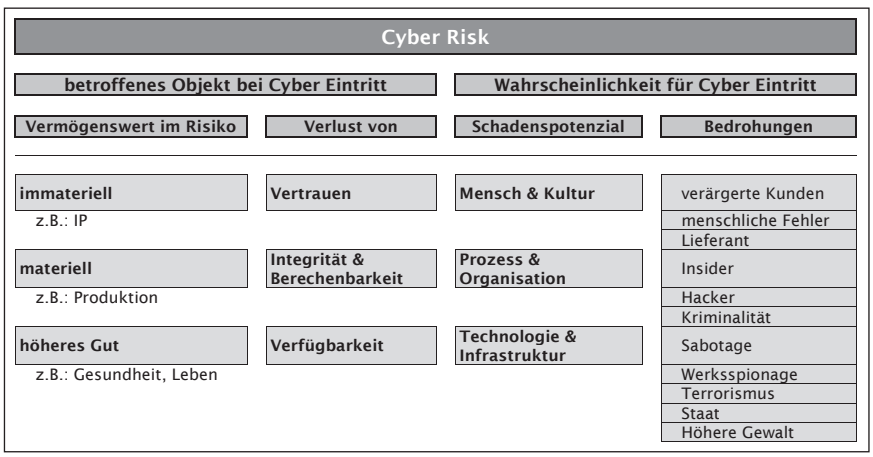

Abb. 1: Beispielhafter Ordnungsrahmen zu Cyber-Risiken

tiert. Gleichzeitig sind aber auch die Risiken, insbesondere Cyber-Risiken, zu bewerten, die damit in Zusammenhang stehen.

Denn inzwischen tangiert jedes solcher Vorhaben, ob Unternehmensbeteiligung, neues Produkt oder neue Produktionsstätte, das Feld der Informations-Technologie, ob produktimmanent (Software, Applikation, etc.) oder Unternehmens-IT (Steuerung, Internet of Things, Industrie 4.0, etc.).

Folglich sind auch solche Vorhaben unter *Cyber Resilience*-Aspekten zu betrachten und auf Cyber-Risiken zu bewerten. Dazu gehören u.a. hineindesignte Sicherheit, Cyber-Risiken von Zulieferern und deren zugelieferten Komponenten, Cyber-Risiken im Laufe des Lebenszyklus, Datenschutz, time-to-market versus Cyber-Sicherheit, etc.

Cyber Resilience betrifft also nicht nur den IT-Verantwortlichen auf C-Level für die eigene IT-Organisation und das zu betreuende IT-System, sondern auch den für das Business Development und Produkt-Entwicklung bzw. für die Produktion verantwortlichen Vorstand.

IV. Leitfaden

Der folgende Leitfaden soll dem Aufsichtsrat aufzeigen, wie die oben abstrakt formulierten Prinzipien konkret umgesetzt werden können und die Cyber-Risiko-Bewertung anhand der Rahmenstruktur vorgenommen werden kann. Dabei sind folgende Methoden anwendbar, um alle zur Bewertung notwendigen Informationen vom zuständigen Management und bei Bedarf aber auch von internen und externen Experten einzuholen:

- Mündliche Befragung (Interview: herausforderndes Proben *(challenging)*)
- Inaugenscheinnahme von IT-Systemen, Orten, Räumlichkeiten und Gegenständen
- Beobachtung (Wahrnehmungen im Rahmen der Vor-Ort- Beurteilung)
- Aktenanalyse bzw. *IT-Dash Board* (hierzu gehören auch elektronische Daten oder statistische Auswertungen wie KPIs, etc.)
- Datenanalyse (z.B. Konfigurationsdateien, Logfiles, Auswertung von Datenbanken, etc.)
- Prozessanalyse (z.B. Prozessbeschreibungen im QMS, etc.)
- schriftliche Befragung (z.B. Fragebogen)
- Protokollierung aller Ergebnisse

Dies klingt im ersten Ansatz wie ein Misstrauensvotum gegenüber dem Vorstand, insbesondere im Falle eigener stichprobenartiger Besichtigungen. Entsprechend sensibel muss der Vorstand davon überzeugt werden, dass auch er ein Interesse an einer solchen gemeinsam durchgeführten regelmäßigen Überprüfung haben muss, denn in der Regel kann und wird er es nicht selbst leisten und stützt sich auf den Bericht des IT-Verantwortlichen.

Der Aufsichtsrat sollte sich daher regelmäßig auf aggregiertem Level durch den Bericht des C-Level-Verantwortlichen *(IT-Dash-Board)* und auch durch stichprobenartige Besichtigungen des internen oder externen IT-Raumes (Rechenzentrum, insourced, outsourced) einen Überblick über den Zustand des IT-Systems und dessen Zugang verschaffen, über wesentliche Veränderungen informiert werden und mittels verständlicher und plausibler KPIs dessen Leistungsfähigkeit bzw. dessen Anfälligkeit bewerten können. Desweiteren muss sich der Aufsichtsrat über die zugrunde liegenden Prozesse wie Datensicherung *(Back-Up)*, Passwort-Philosophie (Änderungsfrequenz, Hinterlegung), physikalische und logische Zugangskontrolle inkl. Protokoll-Datei *(Logfiles)*, Dokumentation im Allgemeinen und von Systemveränderungen im Speziellen *(Configuration Management*: Hardware, Software), Wiederherstellung der Grundfunktionen im Falle eines Totalausfalles *(Disaster Recovery)*, etc. nicht nur regelmäßig informieren, sondern dies plausibel und stets aktuell belegen lassen bzw. sich ggf. selbst davon überzeugen.

Im Rahmen der Bilanzprüfung sollte der Wirtschaftsprüfer regelmäßig mit dem Prüfungsschwerpunkt IT und insbesondere ERP-System beauftragt werden, um Kunden- und Artikelstammdaten sowie Kalkulationsprogramme und -parameter auf Plausibilität und auch auf Manipulation zu überprüfen.

Die IT-Infrastruktur und die zugrunde liegenden Prozesse sollten Teil des Audits des Qualitäts-Management-Systems sein. Die letztgültigen Audit-Berichte geben daher weiteren Aufschluss und sollten zur Plausibilitätsprüfung vom Aufsichtsrat mit einbezogen werden. Das *IT-Dash-Board* sollte neben den KPIs auch eine Statistik über versuchte und gelungene Cyber-Angriffe enthalten sowie Komponenten- und Systemausfälle, wobei zusätzlich Toleranzbereiche mittels Benchmark-Angaben gegeben werden sollten zur Einschätzung und Bewertung der statistischen Daten. Auch simulierte Angriffe *(Penetrations-Tests)* sollten regelmäßig durchgeführt und der Ergebnisbericht vorgelegt und bewertet werden.

Der Aufsichtsrat sollte sich aus dem oben im Schaubild dargestellten Muster des Ordnungsrahmens für Cyber-Risiken einen eigenen Ordnungsrahmen ableiten und damit auf sein Unternehmen angepasst definieren lassen, auf welche betroffenen Objekte er sich besonders fokussieren und welche Eintrittswahrscheinlichkeit er bewerten lassen will. Beginnend mit einem spezifischen Risiko, wird das betroffene Vermögen und die Kategorie des Verlustes untersucht, im Weiteren das Schadenspotenzial und die Bedrohung abgeschätzt, sodass am Schluss die Auswirkung und der mögliche Schaden quantifiziert werden können. Dies sollte für jedes erdenkliche wesentliche Risiko durchgeführt werden.

V. Checkliste

Im Detail werden dazu folgende Checkliste und folgende Dokumente vorgeschlagen, die für einen Auf-

sichtsrat auf aggregiertem Level dieses Monitoring und die Bewertung möglich machen soll.

Prämissen

Folgende Prämissen sollten dabei von Ihnen als Aufsichtsrat beachtet werden:

1. Etablieren Sie ein *Corporate Resilience Committee*, in dem ein versiertes Aufsichtsrats-Mitglied, der IT-Verantwortliche auf C-Level und der für IT verantwortliche Wirtschaftsprüfer vertreten sind.
2. Seien Sie kritisch, Risiken und Sicherheit werden zu häufig unterschätzt.
3. Stellen Sie einfache und präzise Fragen und Nachfragen zur Plausibilität und fordern Sie den IT-Verantwortlichen heraus.
4. Lassen Sie sich die Fragen stets so beantworten, dass sie diese ohne ein detailliertes IT-Verständnis verstehen. „IT-Techies" neigen zu Fremdwörtern, fordern Sie Vereinfachung und erläuternde Beispiele, aus denen die Antwort klar und verständlich wird.
5. Lassen Sie sich auf keine Detail-Diskussion mit dem IT-Verantwortlichen ein, diese verlieren Sie immer!
6. Fordern Sie zu allen Antworten aktuelle Dokumente als Nachweise. IT ist zu schnelllebig und zu *fuzzy*, sorgfältige Dokumentation also ein MUSS.
7. Beauftragen Sie initial eine „IT-Due Diligence", an der Sie auch stichprobenweise persönlich teilnehmen.
8. Lassen Sie stets akribisch entdeckte Schwachstellen dokumentieren, fordern Sie die Behebung innerhalb eines vorgegebenen Zeitintervalls und verfolgen Sie diese.

IT-Infrastruktur

Statt vieler Worte lässt sich das IT-System am besten durch einen Blick auf das Schaubild der aktuellen und vollständigen IT-Infrastruktur erfassen und Änderungen verfolgen. Dieses Schaubild enthält alle Rechenzentren/Datenräume (intern, extern), Server, interne und externe Netzwerk-Verbindungen, Angaben zu Kapazitäten, Auslastungen und Schutzvorrichtungen (MPLS-Leitungen, VPN-Tunnel, Firewall, etc.). Der Aufsichtsrat muss dieses Schaubild nicht im Detail verstehen, aber sich grob und verständlich den Aufbau erklären lassen, mittels KPI die Auslastung/Performance der Server, Netzwerkverbindungen, etc. darstellen lassen, Schwachstellen und Gegenmaßnahmen aufzeigen und erläutern lassen und den geplanten Ausbau des IT-Systems darstellen lassen. Im Einzelnen bedeutet dies:

1. Absicherung von Netzübergängen (Verschlüsselung, Sicherheitsgateways, insb. für mobile Zugänge, etc.).
2. Abwehr von Schadprogrammen (durchgängig, verschiedene Abwehrprogramme, etc.).
3. Inventarisierung der IT-Systeme (nur bekannte und autorisierte Systeme, *Configuration Management*).
4. Datensicherung (*backup*, Häufigkeit, Medium, sichere Aufbewahrung, etc.).
5. Vermeidung von offenen Sicherheitslücken (*updates, patch-Management, workarounds*, etc.).
6. Sichere Interaktion mit dem Internet (*Browser*, E-Mail, abgesicherte *Cloud-Services*, etc.).
7. Logdatenerfassung und -auswertung (regelmäßige Zugangskontrollüberwachung: physikalisch: Datenraum; logisch: Passwörter, etc.).
8. Sicherstellung eines aktuellen Informationsstands (Infos zur Cyber-Sicherheit, Maßnahmen, aktuelle Viren und Angriffe, etc.)
9. Bewältigung von Sicherheitsvorfällen (Prozesse im Schadfall, Übung, etc.).
10. Sichere Authentifizierung (Absicherung kritischer Ressourcen, etc.).
11. Gewährleistung der Verfügbarkeit notwendiger Ressourcen (ausreichende personelle und finanzielle Ressourcen für Cyber-Sicherheit, ext. Dienstleister, etc.).
12. Durchführung nutzerorientierter Maßnahmen (Information, Sensibilisierung der Nutzer, etc.).
13. Sichere Nutzung Sozialer Netzwerke (*social media guidelines*, etc.).
14. Durchführung von Penetrationstests (regelmäßige Penetrationstests, Auswertung und Risiken-Minimierung).

Prozesse

Ein umfassendes und zertifiziertes Qualitätsmanagementsystem beinhaltet eine vollständige Prozessbeschreibung auch der IT-Organisation. Schwerpunkte sollten insbesondere Präventivmaßnahmen sein wie *updates, back-up*, Passwortänderung, etc. (Häufigkeit, Aufbewahrung, etc.), aber auch für den Eintrittsfall eines Risikos die Notfallwiederherstellung *(disaster recovery)* und die Analyse des Einflusses auf den Geschäftsbetrieb *(Business Impact Analysis)*. Im Kontext des *Corporate Resilience* ist allerdings der unterbrechungsfreie Geschäftsablauf durch das Betriebliche Kontinuitätsmanagement *(Business Continuity Management)* umfassender statt des alleinigen *disaster recoveries* des IT-Systems nach einem Ernstfall.

VI. Fazit

Vernetzte IT-System von Unternehmen sind inzwischen erheblich mehr Risiken ausgesetzt als Stand-Alone-Architektur in früheren Zeiten. Aufsichtsräte müssen dies nicht nur im Rahmen des Unternehmens-Risiko-Managements (Enterprise Risk Management) mitbewerten, sondern im Kontext der ganzheitlichen Stärkung der Unternehmens-IT (Cyber Resilience), die über die übliche Cyber-Security hinausgeht. Aufsichtsräte benötigen im Rahmen ihrer Governance-Funktion einen Leitfaden, um diese komplexe Aufgabe zu bewältigen.