NWB Sanieren Nr. 10 vom 29.10.2024

Sanierung im digitalen Zeitalter

Die Bedeutung der IT im Kontext von Sanierungsgutachten nach IDW S 6 – Teil 1: Sanierungsrisiko Cyber-Sicherheit

Prof. Andreas Crone und Prof. Dr. Christian Jung *

In einer Sanierungssituation haben Unternehmer und Sanierer auch und besonders das Thema IT zu betrachten, wozu diese Beitragsreihe verschiedene Teilbereiche der Informationstechnologie aufzeigt. In Teil 1 wird das Sanierungsrisiko Cyber-Sicherheit behandelt – und wie damit umzugehen ist.

KERNAUSSAGEN

- Sanierungsgutachten beleuchten regelmäßig nicht oder zu wenig das Thema Cyber-Sicherheit.
- Fortführungs- und Fortbestehensprognosen ohne individuelle Analyse der IT-Sicherheit und Aussage zur IT-Sicherheit sind nicht aussagekräftig.
- Unternehmer und Sanierer riskieren ohne vollständige Analyse der IT-Sicherheit und der Definition von Abwehrmaßnahmen unmittelbar die Unternehmensexistenz.

I. Einleitung: Die Notwendigkeit der IT wächst – und damit die Risiken

Die fortschreitende Digitalisierung und digitale Transformation sind ein unerlässlicher Prozess. Ohne sie haben die meisten Unternehmen keine Chance der langfristigen Fortführung. Mit der Digitalisierung entstehen jedoch, neben vielen Chancen, auch erhebliche Risiken.

Durch die ansteigende und notwendige digitale Verzahnung der Institutionen, Daten und Prozesse ist nahezu jedes Unternehmen attraktives Ziel einer rasant wachsenden Cyberkriminalität. Angesichts der zunehmenden Bedrohung durch Cyberangriffe, die von Phishing und Ransomware bis hin zu Distributed Denial of Service (DDoS)-Attacken, Social Engineering und einfachem, aber effektivem Passwortdiebstahl reichen, wurde die IT-Sicherheit schon lange zu einem entscheidenden Faktor für die Unternehmensstabilität und deren Fortbestand.

Störungen, wie die Sperrung von Konten oder die Stilllegung von Betriebsanlagen, können kurzfristig die Existenz eines Unternehmens ebenso vernichten wie der oft damit verbundene langfristige Vertrauensverlust, welcher durch erfolgreiche Angriffe, Datenverluste, Datenmanipulation, Veröffentlichung von Daten sowie jegliche IT-Schäden verursacht wird.

II. Trugschluss: „Uns wird es schon nicht treffen“

Besorgniserregend ist die Professionalisierung der Cybercrime-Industrie. Das Geschäftsmodell „Cybercrime-as-a-Service“ ermöglicht es selbst weniger technikaffinen Kriminellen, hochkomplexe Angriffe durchzuführen, indem sie spezialisierte Dienstleistungen von sogenannten Initial Access Brokern einkaufen. Diese Broker verschaffen Zugang zu IT-Systemen und bieten ihre Dienste oft verschiedenen Akteuren an. Infektionen und Angriffe können monatelang unbemerkt bleiben.

Ein zentraler Aspekt moderner IT-Sicherheitsstrategien ist der Schutz vor Ransomware, einer der am schnellsten wachsenden Bedrohungen im Cybercrime-Spektrum. Ransomware-Angriffe, bei denen Daten verschlüsselt und Lösegeldforderungen gestellt werden, können den Geschäftsbetrieb unüberwindbar stören oder zu großen finanziellen Verlusten führen. Phishing-Angriffe, die zunehmend durch Künstliche Intelligenz (KI) verfeinert werden, verstärken zusätzlich die Bedrohung, da sie personalisierte und in der Klangfarbe perfekt abgestimmte Nachrichten versenden, die die Wahrscheinlichkeit eines effektiven Angriffs und die Erbeutung von Zugangsdaten oder geheimen, sensiblen Informationen erhöhen.

Ein weit verbreiteter Irrtum in Unternehmen ist die Annahme, dass sie nicht das Ziel von Cyberangriffen werden können oder dass andere Marktteilnehmer interessanter für Kriminelle sind oder dass man selbst bereits ausreichend geschützt sei. Erweisen sich diese Annahmen als Trugschluss, kann dies existenzielle Folgen bis hin zur Insolvenz des Unternehmens nach sich ziehen. Daher ist dieses Thema bei jeder UnternehmensanalyseS. 285 kritisch zu beleuchten; dies gilt auch in Situationen, in denen sich ein Unternehmen bereits in einer betriebswirtschaftlichen Krise befindet. Der Standard für die Erstellung von Sanierungskonzepten (IDW S 6) [1] greift dieses Thema auf und verweist unter Bezugnahme auf die Voraussetzungen zur Entwicklung und Definition des Leitbildes des sanierten Unternehmens zunächst auf die Bedeutung des Vorhandenseins einer digitalen Strategie, die als entscheidend für ein erfolgreiches Geschäftsmodell und damit für den Sanierungserfolg angesehen wird. Elementare Bestandteile der digitalen Strategie wiederum sind, neben digitalen Absatzmöglichkeiten und digitalen Prozessen, insbesondere Vorkehrungen zur Abwehr von Cyberangriffen. Sind diese nicht vorhanden, können die Zukunftsfähigkeit des Geschäftsmodells und damit auch der Sanierungserfolg signifikant (negativ) beeinträchtigt werden, vgl. IDW S 6, Rz. 66.

Aktuelle Studien [2] des Bundeskriminalamts und des Branchenverbands Bitkom e.V. zeigen durch Cyberkriminalität verursachte Schäden von rund 148 Mrd. € in Deutschland jährlich. Dies entspricht über **134.000 dokumentierten Fällen**, bei einer Dunkelziffer von bis zu 91,5 %. Ob Apotheke, Automobilbauer, Bäckerei, Börse, Großbank, (Online-)Handel, Partei, Anwaltskanzlei, Verein oder Zeitarbeitsbranche: Alle und Jeder ist gefährdet!

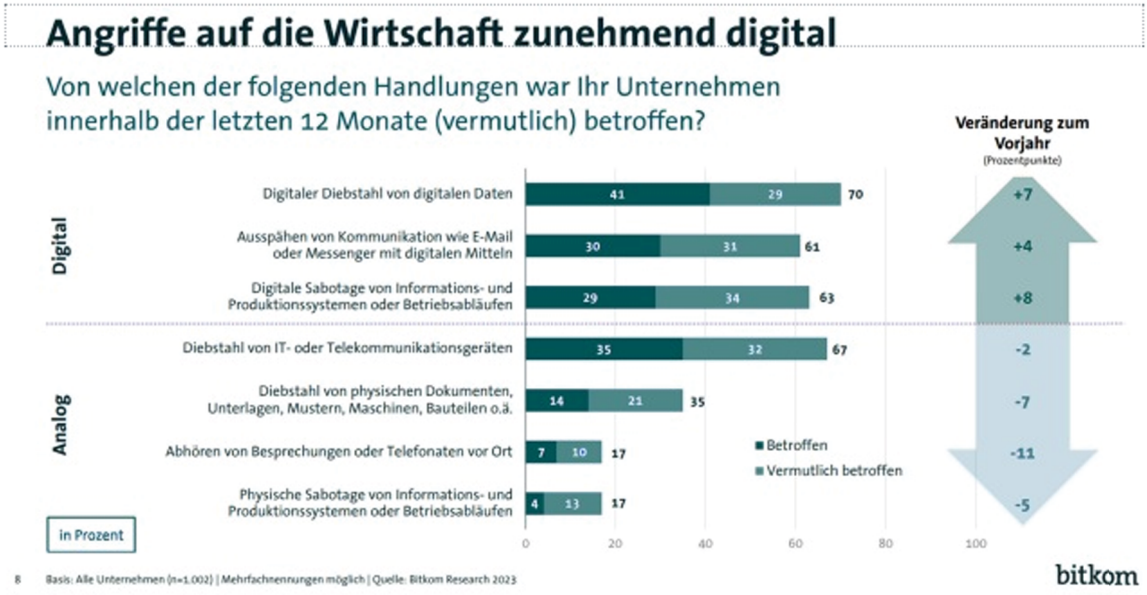

Abb. 1: Angriffe auf die Wirtschaft erfolgen zunehmend digital

Diese alarmierenden Zahlen verdeutlichen die **Notwendigkeit** für Unternehmer und auch Unternehmensberater, dieses Thema ernst zu nehmen, genau zu analysieren und Sicherheitsmechanismen zu implementieren.

III. Es wird uns alle treffen! Und dann?

Experten warnen, es werde **jedes** Unternehmens treffen, da ein „Wettrüsten“ a la Hase und Igel nicht dauerhaft zu gewinnen ist; die Unternehmer also nicht beständig schneller und besser als Kriminelle sein können. Die Software ist nicht sicher und wird es nie sein. Es gibt drei Richtungen des KI-Wettrüstens: KI, um die Sicherheit zu verbessern, KI genutzt durch die Hacker und die Angriffe gegen die KI.

Neben den erwähnten Gesamtwirtschaftsschäden, die durch Cyberangriffe verursacht werden, sehen sich Unternehmen auch mit weiteren gravierenden Folgen konfrontiert. Dazu gehören Vertrauensverlust oder nachlassende Disziplin, Unter- wie Überforderung oder eine erhöhte Fluktuation von Mitarbeitenden, da das Arbeitsumfeld durch zusätzliche Unsicherheit und Stress belastet wird. Gleichzeitig sind meist Lieferanten, Kunden, Banken, Presse usw. betroffen. Regelmäßig kommen Projekte zum Stillstand, da die betroffenen Teams möglicherweise mit dem Wiederaufbau oder der Stabilität der IT- und Betriebssysteme oder Produktionsanlagen kämpfen.

Operative Abläufe werden höchstwahrscheinlich gestört, was insbesondere in einem wettbewerbsintensiven Markt zu erheblichen wirtschaftlichen Einbußen bis hin zum Existenzverlust führen kann. Die Kosten für die Wiederherstellung der IT-Systeme und die Implementierung von verbesserten Sicherheitsmaßnahmen sind meist hoch und lange andauernd. Schließlich kann die mentale Belastung der Mitarbeiter infolge solcher Vorfälle zu erhöhtem Krankheitsstand und damit verbundenen Ausfallzeiten führen, was den Betrieb weiter beeinträchtigt. Negative Auswirkungen auf Reputation und Vertrauen können langfristige Geschäftsbeziehungen gefährden oder zerstören.

Praxishinweis

Erfolgt der Cyber-Angriff, ist es von größter Bedeutung, sofort IT-Abteilung, IT-Spezialisten, externe Berater und die zuständigen Behörden, ggf. Banken und weitere Stakeholder zu informieren. Unterstützung und hilfreiche Ressourcen sind online, wie bspw. beim Bundeskriminalamt (BKA), [3] zu finden, wenngleich die steigende Zahl von Cyberangriffen die staatlichen Sicherheitsbehörden oft noch stärker als die private Cyber-Sicherheitsbranche an ihre Grenzen bringt.

Dann folgt harte Arbeit.

Es ist daher entscheidend, proaktive Strategien zur Cyberabwehr zu entwickeln, um nicht nur die Bedrohungen zu minimieren, sondern auch effektive Notfallpläne zu erarbeiten, die die Reaktion auf einen – ohnehin irgendwann anstehenden – Cyberangriff organisieren, erleichtern und relativ schnell und erfolgreich zu machen haben; also überhaupt ermöglichen.

IV. Relevanz der IT-Sicherheit nach IDW S 6

Um einen Ernstfall mit fatalem Ausgang während und nach einer Sanierung zu vermeiden, fordert IDW S 6 für Sanierungskonzepte eine detaillierte Analyse der Unternehmenssituation. Gemäß Rz. 53 ff. IDW S 6 ist eine, „vollständige Erfassung der für das Unternehmen wesentlichen Daten“ erforderlich, wobei bei den wesentlichen Angaben organisatorische, rechtliche, steuerliche, finanzwirtschaftliche, leistungswirtschaftliche und personalwirtschaftliche Verhältnisse genannt werden. In Abschnitt 3.4 und Abschnitt 4 werden die Themen ESG (Environment, Social, Gouvernance) und IT (weitgehend nur Absatzmöglichkeiten, Geschäftsprozesse und Cyber-Angriffe) etwas stiefmütterlich behandelt. Es wird jedoch hervorgehoben, dass ohne Vorkehrungen zur Abwehr von Cyber-Angriffen die Zukunftsfähigkeit des Geschäftsmodells und damit der Sanierungserfolg signifikant beeinträchtigt werden kann, vgl. IDW S 6, Tz. 66.

Im IDW S 6 ist das Thema Cyber-Sicherheit somit enthalten und damit „sanierungsrelevant“. Im Rahmen der Erstellung von Sanierungsgutachten hat das Thema Cyber-Sicherheit aus den oben beschriebenen Gründen und potenziellen Folgen eine wesentliche Rolle zu spielen, wird allerdings, aus der Erfahrung der Autoren heraus, häufig in Sanierungskonzepten sträflich vernachlässigt oder nur oberflächlich behandelt und weder fundiert noch individuell konstruiert. Stattdessen wird oft mit austauschbaren Textbausteinen das Thema im Gutachten abgehandelt, ohne auf die Spezifika des untersuchten Unternehmens genau einzugehen, was oftmals auch der mangelnden (IT-)Fachkenntnis vieler Sanierungsberater geschuldet ist.

Praxishinweis

IDW S 6 betrachtet das Thema IT-Sicherheit als einen integralen Bestandteil der Sanierungsstrategie. Ein vollständiges Sanierungskonzept muss eine umfassende Analyse der IT-Risiken beinhalten, um sicherzustellen, dass alle relevanten Risiken des Unternehmens identifiziert und angemessen adressiert werden. Darüber hinaus verlangt der Standard die Implementierung eines robusten Risikomanagementsystems, das nicht nur präventive Maßnahmen, sondern auch eine klare Strategie für den Umgang mit potenziellen IT-Sicherheitsvorfällen umfasst.

Also: **Die Relevanz ist gegeben, die richtige praktische Umsetzung geschieht selten.**

V. Wirksamer Schutz – ein vollständiges, tragfähiges Sanierungskonzept

Nachdem Kritikalität, Relevanz und regelmäßig mangelnden Anti-Cyberkonzepten und deren Umsetzung festgestellt sind, gilt es die gemäß IDW S 6 notwendigen Maßnahmen zu definieren und zu implementieren, um damit überhaupt die Grundlage für eine positive Sanierungsaussage zu legen.

Die Erstellung eines Sanierungsgutachtens gemäß IDW S 6 ist unvollständig, wenn das Thema IT-Sicherheit nicht umfassend integriert wird. IDW S 6 fordert ausdrücklich, dass alle relevanten IT-Risiken detailliert analysiert und entsprechende Schutzmaßnahmen implementiert werden. Das Gutachten muss präventive IT-Sicherheitsmaßnahmen sowie Strategien für den Umgang mit potenziellen IT-Sicherheitsvorfällen umfassen, um den Fortbestand des Unternehmens zu sichern. Ohne diese Maßnahmen kann das Sanierungskonzept die Anforderungen des IDW S 6 nicht erfüllen, was den Sanierungserfolg und die langfristige Unternehmensstabilität erheblich gefährdet.

Durch die Kombination u. a. der folgenden Maßnahmen ist ein effektives Verteidigungsnetz gegen Cyber-Angriffe aufzubauen und die Resilienz gegenüber Bedrohungen sicherzustellen.

1. Organisatorische Maßnahmen

Risikobewertung und -management: IDW S 6 betont die Bedeutung eines umfassenden Risikomanagementsystems, welches die IT-Sicherheit einschließt. Ein effektives Risikomanagement sollte nicht nur präventive und reaktive IT-Sicherheitsmaßnahmen, sondern auch strategische Überlegungen sowie die Durchführung einer gründlichen Bewertung beinhalten, um potenzielle Bedrohungen und Schwachstellen zu identifizieren. Diese Einschätzung sollte sowohl interne als auch externe Faktoren umfassen, einschließlich der Analyse von Bedrohungen und Sicherheitsmaßnahmen.

Da Cyber-Bedrohungen sich ständig verändern und weiterentwickeln, ist es unerlässlich, eine proaktive Herangehensweise zu wählen, die nicht nur aktuelle Risiken analysiert, sondern auch zukünftige Bedrohungen und erfolgreiche Angriffe antizipiert. Im Rahmen des Risikomanagements sind die identifizierten Ergebnisse zu priorisieren und geeignete Maßnahmen zur Risikominimierung und -abwehr zu implementieren. Ein kontinuierliches Monitoring-System ist zu etablieren, das regelmäßige Überprüfungen und Anpassungen der Risikomanagementstrategien ermöglicht, um auf Änderungen schnellS. 287 reagieren und drohende Betriebsunterbrechung oder Datenverluste minimieren und Kernfunktionen, Geschäftsprozesse, Infrastruktur und Integrität weitgehend schützen zu können. Die Antworten werden in Neutralität, Reliabilität (Zuverlässigkeit) und Validität gegenübergestellt. Ein Normierungsversuch gegenüber vergleichbaren anderen Untersuchungen ist meist möglich. Mit oder ohne Normierung werden aus den ermittelten Antworten klare und unmissverständliche Aussagen zur Risiko- und monetären Bewertung ermittelt, formuliert und für die Zielgruppe interpretiert bzw. zusammengefasst.

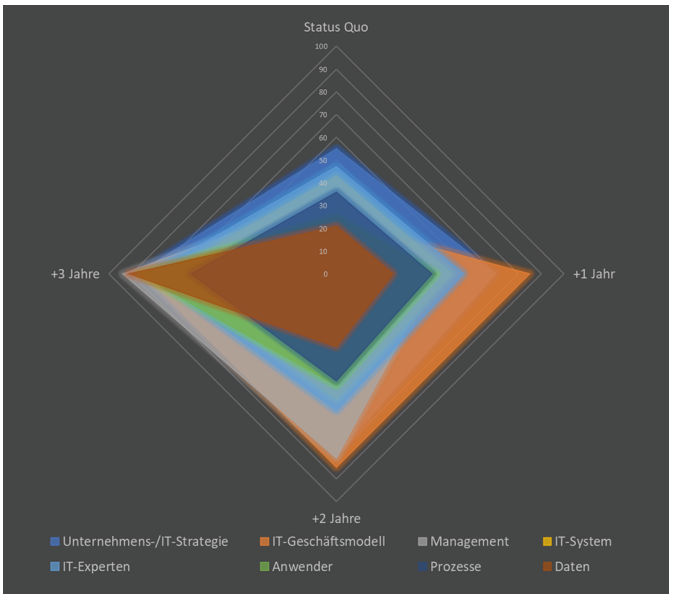

Abb. 2: Grafik: Gradmesser IT-Strategie – Feststellung des Status Quo und Prognose der möglichen Entwicklung über 3 (oder x) Jahre

Sicherheitsrichtlinien: Entwicklung und Um-/Durchsetzung von klaren IT-Sicherheitsrichtlinien und strengem Zugriffsmanagement. Es ist sicherzustellen, dass nur autorisierte Personen auf sensible Informationen zugreifen können.

Notfallplan: Erstellung eines detaillierten, vollständigen und robusten Notfallplans, der die Maßnahmen bei einem Cyberangriff beschreibt, einschließlich Kontaktinformationen und Verfahren zur Eskalation. Dieser Plan sollte klare Zuständigkeiten und Abläufe für die Reaktion auf verschiedene Arten von Cybervorfällen und die Wiederherstellung der Betriebsfähigkeit wie auch die Kommunikation nach innen und außen festlegen. Er ist regelmäßig zu üben!

Sicherheitskultur, Sensibilisierung, Mitarbeiterschulung: Eine Sicherheitskultur ist zu schaffen, die die IT-Sicherheit priorisiert und das Bewusstsein für mögliche Bedrohungen erhöht; z. B. durch regelmäßige, praktisch orientierte Schulungen der Mitarbeiter zum Erkennen und zum Umgang mit Cyberbedrohung und Phishing-Methodik, um das Wissen der gesamten Belegschaft auf dem neuesten Stand zu halten. Regelmäßige Sensibilisierungskampagnen und digitale Erinnerungen stärken ebenso das Bewusstsein.

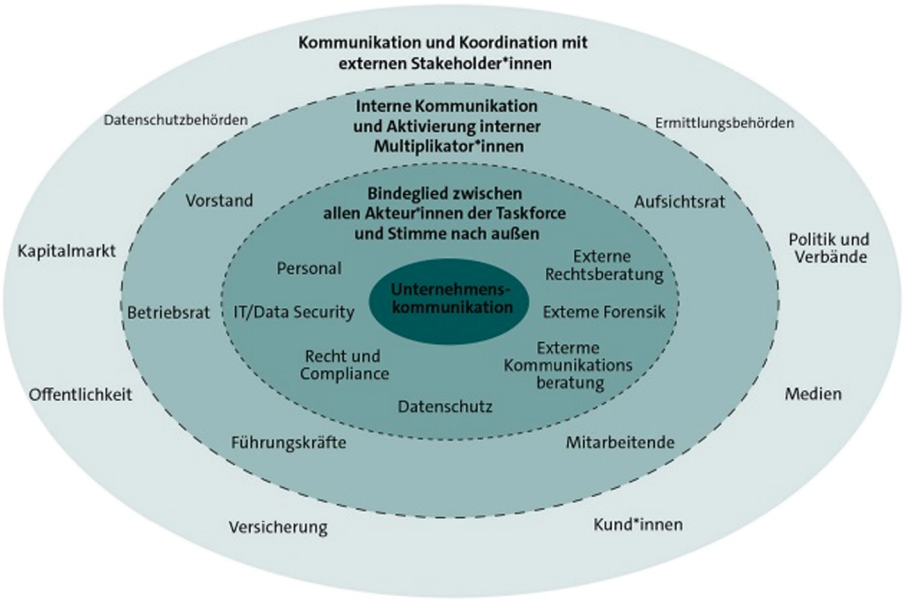

Abb. 3: Kommunikation und Koordination mit Stakeholdern

2. IT-Sicherheitsmaßnahmen

Multi-Faktor-Authentifizierung (MFA): Einführung von MFA für alle Benutzerkonten, um die Sicherheit der Anmeldungen zu erhöhen.S. 288

Verschlüsselung von Daten: Anwendung von Verschlüsselungstechniken für sensible Daten, sowohl im Ruhezustand als auch während der Übertragung.

Firewall und Intrusion Detection Systems (IDS): Implementierung von Firewall und IDS zur Überwachung und dem Schutz des Netzwerkperimeters.

Investition in Sicherheitstechnologie: Regelmäßige Aktualisierung der gesamten IT-Infrastruktur. Dieser Posten kann enorm sein, da die zu sanierende Organisation regelmäßig veraltete oder bereits aus der Wartung gelaufene Produkte im Einsatz haben.

Backup-Strategie und -wiederherstellung: Implementierung robuster Backup-Lösungen, um Daten im Falle eines Angriffs (oder anderer Unregelmäßigkeiten) wiederherzustellen und Betriebsstörungen zu minimieren.

Sicherheitsüberwachung: Etablierung einer kontinuierlichen, modernen und automatisierten Sicherheitsüberwachung und Nutzung von Sicherheitsinformations- und Ereignismanagement-Systemen, um verdächtige Aktivitäten in Echtzeit zu erkennen.

3. Regelmäßige Überprüfung und Anpassung

Feedback-Mechanismen: Implementierung von Feedback-Mechanismen, um aus Sicherheitsvorfällen und Beinahe-Vorfällen zu lernen und die Sicherheitsstrategien kontinuierlich zu verbessern.

Aktualisierung und Anpassung sämtlicher Parameter: Konzeption, Richtlinien, Softwarestände, Schulungen, Methoden, also alle genannten Maßnahmen usw. sind regelmäßig zu prüfen und anzupassen, um den sich ständig verändernden Bedrohungen gerecht zu werden.

Penetrationstests: Offizielle wie geheime Durchführung regelmäßig geplanter Penetrationstests, um Schwachstellen im System zu identifizieren und zu beheben.

Sicherheitsaudits: Regelmäßige offizielle wie verdeckte Audits der Sicherheitsrichtlinien und -praktiken, um sicherzustellen, dass sie den aktuellen Bedrohungen entsprechen.

4. Finanzielle Maßnahmen

Cyber-Versicherung: Ein zunehmend wichtiger Aspekt des Risikomanagements ist die Absicherung durch Cyber-Versicherungen, die unterstützen können, die finanziellen Folgen eines Cyberangriffs zu bewältigen. Im Rahmen der Risikoanalyse gemäß IDW S 6 ist daher zu prüfen, ob eine Cyber-Versicherung sinnvoll ist und in welchem Umfang sie diese Bedrohungen abdeckt. Ein Auslassen der o. g. Maßnahmen erhöht meist die Prämie oder erschwert einen Abschluss.S. 289

Bewertung und Budgetierung: Es ist notwendig, eine gründliche Risikobewertung durchzuführen, um die genannten Maßnahmen sachgerecht zu bewerten. Dabei müssen potenzielle finanzielle Schäden durch Cyberangriffe sowie die Aufwände für Hardware, Software, Implementierung und Beratungsleistungen präzise identifiziert und quantifiziert werden.

Investition: Gut geplant ist noch nicht umgesetzt. Kluge Investitionen in fortschrittliche, autarke Sicherheitslösungen sind konsequent zu tätigen, um die Widerstandsfähigkeit stetig zu erhöhen und Sicherheitslücken kontinuierlich zu schließen – auch und gerade dann, wenn im Sanierungsfall der Schuh überall drückt.

VI. Qualifikation

Es handelt sich bei der IT-Risikobewertung im Rahmen eines Sanierungsgutachtens nicht mehr um eine Küraufgabe, sondern um einen Teil des Pflichtprogramms. Daraus folgt die Notwendigkeit einer sehr hohen fachspezifischen Qualifikation der Berater, die die genannten Maßnahmen festzustellen haben. Dieses Spezial-Know-how weicht von den Kenntnissen der klassischen, meist betriebswirtschaftlich geprägten Sanierungsberater deutlich ab bzw. erfordert zusätzliches Wissen. Die folgende Tabelle zeigt nur diejenigen obligatorischen Qualifikationen eines Spezialisten, die über die eines ohnehin erfahrenen Sanierungsberaters und Konzepterstellers hinausgehen.

Methodisch	Sozial
► Beherrschung von Auditpraxis und Regelkreisen des Auditprozesses nach DIN EN ISO/IEC 27001:2017[4] ► Existenz von IT-strategischer Fitness ► Aussagekräftiges und korrektes Analysieren von komplexen IT-Sachverhalten	► Fähigkeit, prozessuale, betriebswirtschaftliche, strategische und IT-Themen zu moderieren
Fachlich	**Persönlich**
► Gutes Branchen-, Wirtschafts- und Technologie-Know-how; auch und besonders aus IT- und IT-Transformations- und Automatisierungssicht ► Korrekte Interpretation von betriebswirtschaftlichen, prozessualen und IT-Sachverhalten; auch im Zusammenhang von Vorgaben, Normen oder Vorschriften ► Neutrale und zielsichere Einschätzung der Relevanz von spezifischen Rahmenbedingungen ► Scharfsinnige Trennung von obligatorischen, möglichen und überflüssigen IT-Strategien und Funktionen (Strategen statt technikverliebter Geister!) ► ERP-Know-how der vorgefundenen Systeme ► Expertise für IT-Sicherheit und Methodik zur Vermeidung	► Führungsqualitäten (da hier i. d. R. im Team gearbeitet wird) ► Selbständiges Finden der richtigen Vorgehensweise in der zu untersuchenden Organisation ► Gewissenhaftigkeit beim Zusammenführen einer sauberen Dokumentation als Teilpaket „IT“ bzw. IT-Sicherheit, welches später vom Konzeptersteller zu verwerten bzw. einzubinden ist ► Fähigkeit der passenden Sprache für die – i. d. R. eher IT-fernen – Zielgruppen und Berichtsadressaten

Abb. 4: Notwendiges Know-how von IT-Beratern, welches über die „klassischen Skills“ eines eher betriebswirtschaftlich geprägten Sanierungsberaters hinausgehen

Praxishinweis

Da diese Qualifikationen regelmäßig nicht in einer Person vereinigt verfügbar sind, wird abgesehen von einzelnen Sonderfällen meist ein Team (i. d. R. 2 bis 3 IT-Experten) eingesetzt. Das Ergebnis ist also von erfahrenen Spezialisten zu ermitteln, deren Qualifikation sich von denen des klassisch betriebswirtschaftlich geprägten Sanierungsberaters unterscheidet. Diese ergänzen temporär das (Sanierungskonzept-)Team.

VII. Auswirkungen

1. Auswirkung auf die zur Verfügung stehendende Liquidität

Die o. g. Maßnahmen erzeugen regelmäßig enorme, selten überhaupt oder zu gering kalkulierte monetäre und zeitliche Aufwände; also erhebliche Liquiditätsabflüsse und Investitionen.

2. Auswirkung auf die Aussage zur Fortführung und Sanierungsfähigkeit

Die vorstehende Liquiditätswirkung kann die Fortbestehensprognose zunichtemachen bzw. die Durchfinanzierung der Gesellschaft erschweren (fatal wäre, die Aufwände nicht kalkuliert zu haben oder aus Sparsamkeit auf den Cyber-Schutz zu verzichten und das Unternehmen damit ggf. auch nach der eigentlichen Sanierung weiterhin einem unkalkulierbaren Bestandsrisiko auszusetzen).

Eine positive Sanierungsaussage ist bei einem identifizierten, nicht zu kompensierenden Bestandsrisiko nicht möglich. Welcher Stakeholder sollte finanzielle Beiträge leisten, wenn nicht sichergestellt ist, bei allen Unwägbarkeiten, dass das Unternehmen nicht durch Cyberattacken in der Zukunft existenziell vernichtet oder massiv geschädigt wird?

VIII. Fazit

Die Identifikation, Bewertung, Kompensierung und Planung von IT-Risiken, die irgendwann erhebliche Auswirkungen haben werden, sind essenziell. Die Fortführungsprognose, ein zentraler Bestandteil des Sanierungskonzepts nach IDW S 6, bewertet die Fähigkeit eines Unternehmens, seinen Geschäftsbetrieb nachhaltig fortzuführen. Eine positive Fortführungsprognose erfordert eine robuste IT-Sicherheitsstrategie, die den laufenden Betrieb unterstützt, zukünftige Wachstumsstrategien ermöglicht, das Risiko von Betriebsunterbrechungen und Datenverlusten minimiert sowie das Vertrauen von Investoren und anderen Stakeholdern stärkt. Die Autoren betrachten eine positive Fortführungsprognose und eine positive Sanierungsaussage ohne eine solide IT- und IT-Sicherheitsstrategie als nicht belastbar, da die IT-Sicherheitsstrategie nicht nur ein strategisches, technisches, sondern auch überlebenswichtiges Element der Sanierung darstellt.

Eine sachgerechte Beurteilung der Sanierungsfähigkeit ist daher nur möglich, wenn die Situation in Bezug auf Cyber-Sicherheit überprüft und geeignete Maßnahmen definiert und eingepreist werden.

Unzureichend behandelte IT-Sicherheit erhöht dagegen das Unternehmensrisiko, was zu einem sofortigen oder schleichenden Exitus des Unternehmens führen kann. Eine umfassende Analyse der Situation, die die IT-Infrastruktur und die damit verbundenen Risiken, insbesondere die Abwehr von Cyber-Angriffen, berücksichtigt, ist unerlässlich.

AUTOREN

Prof. Andreas Crone
ist Wirtschaftsprüfer/Steuerberater, Dipl.-Kfm., und berät in eigener Praxis mittelständische Unternehmen, Insolvenzverwalter, Banken und Investoren in Turnaround- und insolvenznahen Situationen. Er ist zugleich geschäftsführender Gesellschafter der Rhein-Neckar-Saar Treuhand Wirtschaftsprüfungsgesellschaft, Mannheim.

Prof. Dr. Christian Jung
ist IT- und Unternehmensberater, Dipl. Ing. der Technischen Informatik, und berät und auditiert internationale Konzerne und Mittelstand in kritischen IT- und Logistik-Situationen, bei Kauf/Verkauf von Unternehmen(steilen). Er ist CEO/CIO der it[colos]AG und Honorar-/Gast-Professor für Digitale Transformation an mittel- und osteuropäischen Hochschulen.

Fundstelle(n): NWB Sanieren 10/2024 Seite 284 - NWB TAAAJ-77211