A. Haftungsfalle Cybercrime

A.1. Einleitung – Haftungsfalle Cybercrime

Axel Anderl/Nino Tlapak

A.1.1. Problemaufriss

„If you are looking at this page right now, that means that your network was successfully breached. All of your files, databases, application files etc were encrypted with military-grade algorithms. If you are looking for a free decryption tool – there is none. For decryption, please write an e-mail to…".

Wenn Sie in Ihrem Unternehmen ein unscheinbares .txt File mit dieser oder einer vergleichbaren Nachricht vorfinden, ist der Worst Case eingetreten – Sie wurden Opfer einer Cyberattacke. Ihre Daten und wesentlichen Informationen sind ganz oder teilweise verschlüsselt und nicht mehr zugänglich. Produktionsmaschinen stehen still, Einkäufe über Ihren Webshop sind unmöglich und Ihre Kommunikationskanäle – von E-Mail bis VOIP – sind lahmgelegt. Solche Attacken sind regelmäßig mit Lösegeldforderungen unter bewusst knapper Fristsetzung, meist 24 bis 48 Stunden, verbunden, um den ohnedies auf allen Ebenen spürbaren Druck weiter zu erhöhen. Um ungehindert agieren und möglichst viele Daten verschlüsseln zu können, erfolgen die Attacken regelmäßig über das Wochenende oder an Feiertagen. Am ersten Werktag danach ist das Unternehmen sehr rasch mit Nachfragen von Mitarbeitern, Kunden und Geschäftspartnern konfrontiert.

Als Konsequenz eines Cyberangriffs sind binnen weniger Stunden wesentliche rechtliche, organisatorische und technische Entscheidungen zu treffen, um den Betrieb aufrechtzuerhalten oder wieder aufzunehmen, Schäden einzudämmen und auch die gesetzlichen Meldepflichten einhalten zu können. Dabei ist jeder Schritt für die nachgelagerte Frage der straf- und zivilrechtlichen Verantwortlichkeit und Haftung wesentlich. Das Um und Auf ist daher die sorgfältige Vorbereitung im Rahmen der Prävention, um dem zunehmenden Risiko durch Cyberangriffe angemessen zu begegnen.

A.1.2. Zunahme und Konsequenzen der Gefahr an Cyberbedrohungen

A.1.2.1. Weltweiter Anstieg an Cyberangriffen

Die Bedrohung durch Cyberattacken ist längst nicht mehr bloß theoretisch oder auf bestimmte Branchen beschränkt: Cyberangriffe wurden schon 2022 als eines der drei größten Geschäftsrisiken identifiziert. Das gilt auch für Österreich: 63 % nennen Cybervorfälle und dabei allen voran Ransomware-Angriffe als bedeutendste Ursache für Betriebsunterbrechungen.[1] Dies ist kein Zufall, sondern Ergebnis eines sich seit 2020 abzeichnenden Trends. Die fortschreitende Digitalisierung führt dazu, dass immer mehr Unternehmen komplexe automatisierte Systeme

1 S jeweils *Allianz Global Corporate & Specialty (AGCS)*, Allianz Risk Barometer 2022, Pressemitteilung vom 18. 1. 2022; für Deutschland zB *brand eins*, Cybersicherheit in Zahlen 2022, 46; generell nimmt die Anzahl der Angriffe zu, vgl *Bundesamt für Sicherheit in der Informationstechnik*, Die Lage der IT-Sicherheit in Deutschland 2022, 67.

im Einsatz haben. Das erhöht zwangsweise das Risiko, Angriffen ausgesetzt zu sein.[2] Das wurde durch die COVID-19-Pandemie und dem Aufkommen von Home Office noch weiter verstärkt. Die kurzfristige Verlagerung zahlreicher Arbeitsplätze sowie die durch die Dezentralität schlechtere interne Kommunikation hat zu einer Verringerung der IT-Sicherheit und zu neuen Sicherheitslücken geführt. Diese werden auch heute noch laufend ausgenutzt:

Ransomware-Attacken sind oft Ausläufer von vergangenen, erfolgreichen Social Engineering-, Brute Force- oder Phishing-Angriffen. Dabei werden entweder mit klassischen Passwort-Crackern oder über personalisierte, täuschend echte E-Mails, Social-Media-Kanäle wie auch klassische Telefonanrufe Passwörter und Zugangsdaten zu Systemen herausgelockt und anschließend missbraucht. Parallel dazu ist – durch den Krieg in der Ukraine stark befeuert – eine drastische Zunahme von staatlichen bzw staatlich unterstützten Attacken zu verzeichnen.[3] Aber auch klassische CEO-Fraud-Angriffe haben während dem Home Office deutlich zugenommen und sind seither weiter auf hohem Niveau. Die Täter erheben dafür mittlerweile regelmäßig durch Hacking-Angriffe im Vorfeld für den Betrug zweckdienliche Informationen und Daten wie zB bestehende Geschäftsbeziehungen oder interne Zuständigkeiten.[4, 5, 6]

Initial Infection Vector, 2021 (*When Identified*)

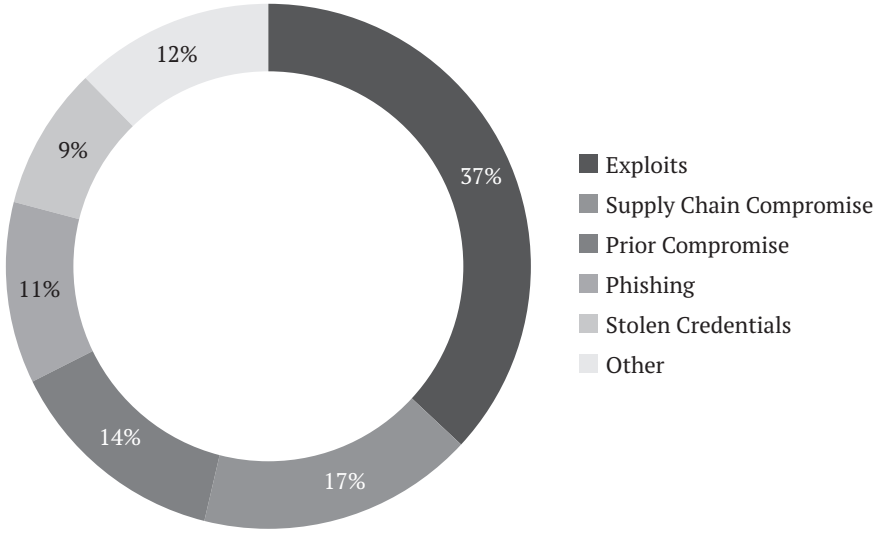

Abbildung 1: Initial Infection Vector, 2021 (When Identified)

Auch die Politik hat die stark zunehmende Gefahr von Cyberangriffen erkannt: Zum Zeitpunkt der Drucklegung befindet sich ein Gesetzesentwurf in Begutachtung, mit dem die Strafdrohungen für reine Cybercrime-Delikte (zB widerrechtlicher Zugriff auf ein Computersystem oder Miss-

2 Vgl zB *FMA*, Digitalisierung am österreichischen Finanzmarkt (April 2022), 21, die aufgrund breiter Online-Angebote von Banken eine umso größere Bedrohungslage erkennt.
3 S jeweils *KPMG/KSÖ*, Studie Cybersecurity in Österreich 2021, 18.
4 *Bundeskanzleramt*, Bericht Cybersicherheit 2020, 39.
5 Zu den wichtigsten Begehungsformen von Cyberangriffen im Detail s Kapitel B.
6 *M-Trends Report 2022*, https://www.mandiant.com/m-trends.

brauch von Computerprogrammen oder Zugangsdaten) von bislang regelmäßig nur maximal sechs Monaten Freiheitsstrafe auf zwei Jahre angehoben werden sollen.[7] In der Praxis werden diese Delikte zumindest bei den besonders brisanten Ransomeware-Angriffen jedoch regelmäßig durch qualifizierte Vermögensdelikte, wie zB Erpressung,[8] überlagert und spielen daher nur eine untergeordnete Rolle. Ob der Täter der gerichtlich verfolgt werden kann, ist freilich eine andere Frage.[9]

A.1.2.2. Ursachen und Auswirkungen

Die seit Jahren steigende Anzahl an Cyberangriffen hat mehrere Ursachen: So wie sich die klassische Leistungserbringung im Online-Bereich vom Outsourcing und customized Lösungen hin zur Cloud und Software-as-a-Service (SaaS) entwickelt hat, ist auch bei Cybercrime eine zunehmende Arbeitsteilung und Vernetzung der Tätergruppen – man kann bereits von Cybercrime-as-a-Service (CaaS) sprechen – zu beobachten.[10] Das erschwert nicht nur die ohnedies sehr unwahrscheinliche Ausforschung der Täter,[11] sondern auch die Vorbereitung der Unternehmen: Die Angriffe sind mittlerweile zunehmend auf die wirtschaftliche Leistungsfähigkeit und vorhandene IT-Infrastruktur mitsamt zugehörigen Backup-Lösungen maßgeschneidert. Die dafür notwendigen Kenntnisse resultieren, wie bereits erwähnt, regelmäßig aus der meist monatelang vor der eigentlichen Verschlüsselung und Lösegeldforderung erfolgten Ausspähung der Systeme der Opfer.[12] Die Kombination aus der hohen, allgemeinen Eintrittswahrscheinlichkeit einem Cyberangriff zum Opfer zu fallen und dem drohenden massiven Schaden führt im Ergebnis zu einem hohen Gesamtrisiko für alle Unternehmen, deren Tätigkeit entweder von Daten oder (internen wie externen) IT-Systemen abhängig ist. Unter Beachtung der in den letzten Jahren in allen Bereichen bis hin zur Industrie rasch vorangeschrittenen Digitalisierung, bleibt daher kaum ein Bereich des (wirtschaftlichen) Lebens außen vor. Die Frage in der Praxis ist daher nicht, ob ein Unternehmen betroffen sein kann, sondern vielmehr wann und in welcher Intensität dies der Fall sein wird. Das zeigt sich schlussendlich auch am stetig steigenden Markt für Versicherungslösungen für Cyberrisken und den diesbezüglich zunehmenden Einschränkungen: So erfolgt die Prüfung der vom Unternehmen gesetzten Präventionsmaßnahmen durch die Versicherung im Vorfeld einer Polizzierung zunehmend strenger. Zudem wurden im Laufe der letzten beiden Jahre die Deckungssummen und -fälle angesichts des gestiegenen Risikos weiter eingeschränkt. Auch im Anlassfall erfolgt schließlich eine genaue Prüfung, ob das Unternehmen seine Präventionspläne laufend aktualisiert und dann auch effektiv umgesetzt hat. Ist das nicht der Fall, entfällt die Versicherungsleistung oder wird drastisch reduziert.[13]

A.1.2.3. Handlungsbedarf als Konsequenz

Die Konsequenz des Anstiegs von Cyberangriffen ist ein akuter Handlungsbedarf auf technischer und organisatorischer Ebene. Aufgrund des stetig wachsenden Risikos über alle Branchen hinweg

7 ME/253 27. GP.
8 §§ 144 iVm 145 Abs 2 StGB: Strafdrohung zehn Jahre bei Gewerblichkeit.
9 S Kapitel D.5.
10 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2020, 11. S auch im Detail Kapitel G.3.
11 S dazu Kapitel D.5.
12 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2020, 16. S auch Kapitel B.
13 S Kapitel C.10.

sollten sich vor allem Entscheidungsträger in Unternehmen strategisch mit diesem Thema befassen und dieses nicht (wie in der Vergangenheit) gänzlich den IT-Abteilungen überlassen.[14] Die Komplexität der Situation ergibt sich in der Praxis aus dem Gesamtbild des Bedrohungsszenarios:

- Unbekannte Täter mit variierender Vorgehensweise und Motiv:
  - Fehlende Vorhersehbarkeit des Eintritts der angedrohten Konsequenzen bei Nicht-Zahlung des Lösegelds;
  - Keine Sicherheit der Rückerlangung sämtlicher Daten und Löschung durch die Täter bei Zahlung;
  - Gefahr neuerlicher Angriffe auch bei Zahlung.
- Mannigfache potenzielle Einfallstore:
  - Fehlende Awareness bei Mitarbeitern;
  - Einsatz veralteter, weil historisch gewachsener Systeme;
  - Sicherheitslücken bei Vertragspartnern, Service Providern oder sonstigen Dritten;
  - Bewusste interne Schadenszufügung (Insider Threats).
- Komplexe, dezentralisierte IT-Landschaft;
- Hoher individueller Beratungsbedarf;
- Zahlreiche, in unterschiedlichen Normen, Verordnungen und Gesetzen verstreute Sorgfalts- und Meldepflichten
- Praktische Schwierigkeiten bei der Bewertung und Berechnung der im Anlassfall eingetretenen Schäden:
  - Fehlende historische Dokumentation;
  - Schaden durch Produktionsausfall vs entgangener Gewinn;
  - Reputationsschäden;
  - Verlust von Know-how, Betriebs- und Geschäftsgeheimnissen;
  - Potenzielle Verwaltungsstrafen und zivilrechtliche Schadenersatzansprüche.

Aufgrund der Intensität der Folgen eines Cyberangriffs ist es im Sinne der unternehmerischen Sorgfaltspflicht und zur Aufrechterhaltung eines weitgehend friktionsfreien Betriebs geboten, vorab ein konzises Präventionskonzept sowie einen detaillierten Handlungsleitfaden für den Anlassfall auszuarbeiten. Während die tatsächlich zu setzenden, effektiven Maßnahmen vom jeweiligen Business Concept, technischem und organisatorischem Umfeld sowie Unternehmenskultur abhängen, sind die folgenden Voraussetzungen in jedem Fall zu schaffen:[15]

- ✓ Prüfung und Dokumentation des Status Quo der etablierten Sicherheitsmaßnahmen;
- ✓ Aufarbeitung anwendbarer rechtlicher Vorgaben, wie insb Meldepflichten samt Fristen;
- ✓ Aufarbeitung und Schließung bei der Prüfung erkannter Lücken;
- ✓ Erstellung eines maßgeschneiderten Präventionskonzepts inkl Leitfaden für den Ernstfall sowie Schulungen für Mitarbeiter;

14 *brand eins*, Cybersicherheit in Zahlen 2022, 31.
15 S im Detail Kapitel C.3. sowie Kapitel C.4.

- ✓ Schaffung von Awareness und Sensibilisierung sämtlicher Mitarbeiter;
- ✓ Sicherstellung der Verfügbarkeit der notwendigen internen wie externen Ressourcen für den Anlassfall.

Die präventiv gesetzten Schritte sind auch sorgfältig zu dokumentieren. Das dient dazu, die Unternehmensführung bei einem etwaig dennoch eingetretenen Vorfall zu entlasten sowie Strafen und Schadenersatzansprüche zu verhindern bzw zu mitigieren.

Praxistipp:

Eine Auseinandersetzung mit der stetig steigenden Bedrohung durch Cyberattacken ist zwingend notwendig. Der Fokus von Unternehmen sollte neben den erforderlichen technischen und organisatorischen Sicherheits- und Präventionsmaßnahmen auch auf der Auf- und Vorbereitung der rechtlichen Dokumentations-, Informations- und Meldepflichten liegen. Für den Anlassfall ist zudem ein klarer, leicht verständlicher und zugänglicher (bestenfalls auch ausgedruckter) Handlungsleitfaden auszuarbeiten, der nicht nur die wichtigsten Schritte samt zugehöriger Fristen, sondern auch die erforderlichen internen wie externen Experten samt Notfallkontaktdaten enthält.

A.1.3. Wichtigkeit der (unterschätzten) Präventionsarbeit

A.1.3.1. Einhaltung der Sorgfaltspflichten

Die für den Vorstand oder die Geschäftsführung wesentliche Frage der Wahrscheinlichkeit und Höhe einer Haftung für die Folgen aus einem erfolgreichen Cyberangriff steht und fällt mit der vorab geleisteten Präventionsarbeit und ihrer Dokumentation. Das ergibt sich nicht zuletzt aus zahlreichen rechtlichen Sorgfaltspflichten:

- Sorgfalt eines ordentlichen Unternehmers (§ 347 UGB, § 25 GmbHG, § 84 AktG);[16]
- Pflicht zur Einrichtung eines internen Kontrollsystems (§ 22 GmbHG, § 82 AktG);[17]
- Gewährleistung eines dem Risiko angemessenen technischen (Datens)Schutzniveaus (Art 32 DSGVO, § 17 NISG);[18]
- Branchenspezifische Sonderanforderungen (TKG, BWG, WAG, BörseG, VAG, GTelG etc);[19]
- Spezifische, zusätzliche Obliegenheitspflichten:
  - Einhaltung der Vorgaben aus Zertifizierungen (zB ISO, ÖNORM);
  - Vertragliche Pflichten (zB gegenüber der Cyberversicherung oder sonstigen Geschäftspartnern).[20]

16 S Kapitel E.3.
17 S Kapitel C.5.
18 S Kapitel C.2. sowie Kapitel C.6.
19 S Kapitel C.7., Kapitel C.8. sowie Kapitel C.9.
20 S Kapitel C.10.

Ob der Angreifer eine am Markt bekannte, im Unternehmen aber nicht geschlossene Sicherheitslücke genutzt hat oder zahlreiche, komplexe IT-Sicherheitsmaßnahmen mit größerem Aufwand umgehen musste, kann am Ende des Tages haftungsrelevant sein. Eine fehlende Vorbereitung für den Worst Case zieht sich als potenzieller Haftungsfall wie ein roter Faden durch sämtliche Bereiche: Eine missachtete Sorgfaltspflicht führt zur zivil- und strafrechtlichen Haftung der Geschäftsführung. Dies kann sowohl Ersatzforderungen von Gesellschaftern oder Aktionären, aber auch von Vertragspartnern auslösen, sofern auch ihre Daten mitbetroffen und damit vereinbarte Geheimhaltungspflichten verletzt wurden.[21] Die Wahrscheinlichkeit von Verwaltungsstrafen durch zuständige Behörden – allen voran der Datenschutzbehörde – steigt, während die potenzielle Deckung durch die Versicherung sinkt, je höher der Sorgfaltsverstoß war. Zudem wird bei Nachlässigkeit als Grund für den Erfolg des Angriffs die Argumentation der Zulässigkeit der Zahlung einer Lösegeldforderung – so sie überhaupt Sinn macht und in Erwägung gezogen wird – erheblich erschwert.[22] Etwaige durch den Angriff geleakte Informationen können zu einem massiven Vertrauensverlust und damit einhergehend zu Reputationsschäden führen, die schlussendlich in einem Kunden- und damit Geschäftsverlust gipfeln.[23]

Die Vorbereitung des Unternehmens auf das reale und stetig steigende Risiko eines Cyberangriffs ist daher nicht nur zu empfehlen, sondern faktisch und rechtlich geboten. Dabei ist je nach Struktur, Kultur und Aufbau des Unternehmens ein breites, maßgeschneidertes Maßnahmenpaket zu etablieren:

A.1.3.2. Mindestumfang der Präventionsmaßnahmen

Vor dem Hintergrund der Hintanhaltung von (erfolgreichen) Cyberattacken und ähnlichen Datenschutzvorfällen sieht Art 32 DSGVO auszugsweise vor, dass *„geeignete technische und organisatorische Maßnahmen"* zu treffen sind, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die konkreten Aktivitäten sollen unter Berücksichtigung (i) des Stands der Technik, (ii) der Implementierungskosten, (iii) der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie (iv) der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos ausgewählt und gesetzt werden.[24] Die DSGVO listet dabei bewusst keine konkreten Maßnahmen auf. Vielmehr muss jedes Unternehmen auf Basis seiner konkreten Risiko- und Gefährdungssituation selbst ein maßgeschneidertes Konzept entwickeln, das im Ergebnis Cyberangriffe den Umständen entsprechend angemessen verhindern kann oder zumindest entsprechend erschwert. So kann in der Praxis bereits ein offensives und transparentes Sicherheitsmanagement – zB eine oder mehrere Sicherheitszertifizierungen, die entsprechend kommuniziert werden – eine präventive und abschreckende Wirkung auf (manche) Angreifer haben.[25] Dabei ist aber gleichzeitig darauf zu achten, die Detailinformationen dazu geheim zu halten, um Angreifern keine Anleitung zu geben.

---

21 S Kapitel H.2.

22 S Kapitel E.3.

23 Zum richtigen Umgang durch die Kommunikation s Kapitel F.2.

24 S im Detail Kapitel C.2.

25 *Jost* in *Pachinger*, Datenschutz – Recht und Praxis (2019). Die risikobasierte Umsetzung von Datensicherheitsmaßnahmen in der Praxis von Unternehmen und Behörden Rz 13.

Aus den Erfahrungen der letzten Jahre können folgende Maßnahmen und Leitlinien unabhängig von der Ausrichtung des Unternehmens als Basis einer Cyberabwehr herangezogen werden. Sie sind im Bereich Datensicherheit etablierte Standards:[26]

- Das IT-Grundschutz-Kompendium[27] des deutschen Bundesamts für Sicherheit in der Informationstechnik („BSI“);
- Das Österreichische Informationssicherheitshandbuch;[28]
- Aktuelle Informationen und Guidelines:
  - Des BSI;[29]
  - der Agentur der Europäischen Union für Cybersicherheit („ENISA“);[30]
  - des US-amerikanischen Instituts für Standards und Technologie.[31]

Abseits der technischen Vorbereitung mit Fokus auf exponierte und kritische Systeme, ist auch das Setzen von organisatorischen Maßnahmen unumgänglich. Dabei stehen die Erstellung, Implementierung und laufende Aktualisierung interner Richtlinien im Vordergrund. Die Mitarbeiter sind sodann zu ihrer Einhaltung zu verpflichten. Dies ist regelmäßig und nicht bloß oberflächlich zu überprüfen. Hintergrund ist, dass selbst die strengsten Passwortvorgaben oder ein etabliertes Berechtigungskonzept nur wenig Erfolg haben können, wenn die Mitarbeiter beim Umgang mit der betrieblichen IT die erforderliche Sorgfalt und Awareness vermissen lassen. Schließlich liegt der Ursprung zahlreicher erfolgreicher Cyberattacken darin, dass Angreifer durch Phishing-Mails oder Social Engineering Zugangsdaten und Informationen erlangen. Aus unserer praktischen Erfahrung haben sich folgende allgemein gültige technische, personelle und organisatorische Grundmaßnahmen als wesentliche Erfolgsfaktoren erwiesen:[32]

- Sensibilisierung im Unternehmen auf potenzielle Cyberangriffe und -risiken, wie zB Anweisung, keine Links aus nicht vertrauenswürdigen E-Mails anzuklicken; keine Anhänge von unbekannten Empfängern zu öffnen; Überprüfung des Absenders (seiner E-Mail-Adresse) bzw kritisches Lesen des Mails auf Plausibilität, Rechtschreibfehler und Authentizität (kommuniziert der vermeintliche Absender wirklich so); Anweisung, bei Unsicherheit Mails vor Klicken auf einen Link oder Öffnen eines Anhangs von der IT überprüfen zu lassen;
- Implementierung, Prüfung und Aktualisierung interner IT- und Compliance-Richtlinien und Arbeitsanweisungen;
- Etablierung eines Krisenplans;
- Implementierung von Virenschutzprogrammen und Firewalls;
- Prüfung möglicher Einsatzbereiche und Implementierung von Verschlüsselungsmechanismen;

---

26 Ua den Standard für Informationssicherheit ISO/IEC 2700, ISO/IEC 27002, ISO/IEC 27018.

27 S https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html (Edition 2023).

28 S https://www.sicherheitshandbuch.gv.at/.

29 S https://www.bsi.bund.de/DE/.

30 S https://www.enisa.europa.eu/.

31 S https://www.nist.gov/.

32 Im Detail s Kapitel C.3. sowie Kapitel C.4.

- Forcierung von Passwortschutz, inkl Prüfung der gelebten Praxis;
- Regelmäßige (off-line) Backups und entsprechende Recovery Tests;
- Penetrations- und Notfalltests;
- Etablierung angemessener Logging-Technologien, um einen potenziellen Datenabzug ausschließen bzw zumindest feststellen zu können;
- Prüfung und Forcierung der Durchführung von regelmäßigen Updates und Systemaktualisierungen;
- Kombination aus physischer Zutritts- und technischer Zugriffsbeschränkung.

Neben der Evaluierung der konkret erforderlichen Präventionsmaßnahmen, ihrer Implementierung sowie laufenden Überprüfung und Aktualisierung ist auch eine nachvollziehbare Dokumentation als Vorbereitung für den Anlassfall nicht zu unterschätzen:

A.1.3.3. Lückenlose Dokumentation der ergriffenen Maßnahmen

Nach einem erfolgreichen Angriff ist zur Haftungsvermeidung für sämtliche haftungsgeneigte Bereiche ein Nachweis zu erbringen, dass im Unternehmen ein effektives, dem Risiko angemessenes und dem Stand der Technik entsprechendes Präventionskonzept implementiert und auch faktisch gelebt wurde. Bloße Behauptungen, Indizien oder Vermutungen sind dafür nicht ausreichend. Vielmehr ist sowohl hinsichtlich der internen Entscheidungsfindung als auch gegenüber der Versicherung, Vertragspartnern und zu guter Letzt gegenüber den zuständigen Aufsichtsbehörden nachzuweisen,

- ✓ welche Maßnahmen,
- ✓ in welchen Bereichen,
- ✓ warum und wie etabliert wurden, sowie
- ✓ weshalb diese den Angriff nicht verhindern konnten,
- ✓ welche Notfallmaßnahmen unverzüglich getroffen wurden und
- ✓ welche zusätzlichen Maßnahmen nun als Konsequenz der Attacke angemessen und zu implementieren sind.

In der Praxis ist oftmals der Nachweis, dass ausgerollte Unternehmensrichtlinien auch eingehalten und geprüft werden, schwierig zu erbringen. Damit das gelingt, bedarf es im Unternehmen einer dokumentierten, klaren internen Rollenverteilung und etablierte Berichtslinien, die über (interne wie externe) Audits kontrollierbar sind. Dabei ist aber gleichzeitig auch besondere Vorsicht geboten: Etwaige bei Audits festgestellte Findings, insb kritische und schwere Gaps, sind ernst zu nehmen und rasch zu schließen. Die Dokumentation darf gerade in solchen Fällen keine Lücken nahelegen. Die Aufarbeitung von Prüfergebnissen ist daher besonders genau festzuhalten. Die zuständigen Behörden sind diesbezüglich sensibilisiert. Sie gehen an die Beurteilung der Präventions- und Abwehrmaßnahmen mit mittlerweile einiger Erfahrung und Fingerspitzengefühl heran. Das Vorweisen kritischer Prüfergebnisse ist daher per se kein Nachteil, so dies in Kombination mit der Umsetzung der empfohlenen Abwehrmaßnahmen dokumentiert ist. Vielmehr zeigt dies die Ernsthaftigkeit der Auseinandersetzung des Unternehmens mit dem Risiko. Kritischer ist, wenn ein Unternehmen keine Prüfungsergebnisse vorlegen kann oder aufgedeckte Schwachstellen nicht oder nicht mit dem notwendigen Nachdruck umgesetzt wurden.