Deutscher Fondsverband

BVI-Leitfaden für Cybersicherheit

Informationssicherheit in der Fondswirtschaft

Vorwort

Cyberkriminalität verursacht immer größere Schäden in der globalen Volkswirtschaft. Schätzungen gehen von weltweit jährlich 600 Milliarden Dollar aus[1]. Die Angreifer werden immer professioneller, sowohl was die Organisationsstruktur als auch die Qualität der Angriffe betrifft.

Technologie verändert auch das Asset Management in einer nie dagewesenen Geschwindigkeit und Größenordnung. Das globale regulatorische Umfeld für Cyber-Sicherheit und Datenschutz wird immer komplexer und fragmentierter. Dies schafft zusätzliche Themen, die höchste Aufmerksamkeit in allen Unternehmen erfordern.

Die im BVI vertretenen Unternehmen haben dieses Papier verfasst, um einen Überblick über die wichtigsten Cyberrisiken für die Fondswirtschaft zu geben, Leitlinien für die Maßnahmen anzubieten, die Fondsgesellschaften und ihre Dienstleister ergreifen können, um sich vor Cyberangriffen zu schützen und den Austausch von Erkenntnissen zur Vermeidung von Cyberrisiken innerhalb der Fondswirtschaft zu fördern.

Zum einen sind Cyberangriffe real und betreffen eine wachsende Zahl von Unternehmen, unabhängig von der Branche. Banken und Versicherungsunternehmen haben dies bereits schmerzlich erfahren. Auch Kapitalverwaltungsgesellschaften sind nicht immun gegen solche Angriffe und könnten angesichts der immens hohen Fondsvermögen zu einem attraktiven Ziel von Cyberattacken werden. Ein öffentlich bekannt gewordener Cyberangriff, beispielsweise mit Datenverlusten, kann zu einem Vertrauensverlust mit hohem Schaden für den Ruf des betroffenen Unternehmens führen. Integritätsprobleme können schnell existenzbedrohend werden, egal ob sie aus Unkenntnis oder aus Fahrlässigkeit aufgetreten sind.

Zum anderen konzentrieren sich nationale und internationale Gesetzgeber sowie die BaFin zunehmend auf die Cyber-Widerstandsfähigkeit der von ihnen beaufsichtigten Unternehmen. Die BaFin erklärt das Handlungsfeld „IT-Aufsicht und Regulierung“ zu einem ihrer Schwerpunktthemen 2019 und gibt deutlich ihre Erwartung zu verstehen, dass die beaufsichtigten Unternehmen alle notwendigen Maßnahmen treffen, um Verstöße zu verhindern.

Hierfür will die BaFin mit umfangreichen Sicherheitstests die IT-Sicherheitssysteme der Unternehmen prüfen[2]. Bei der Untersuchung der BaFin wird es auch darum gehen, wie Krisenübungen und ein wirksames Notfallmanagement bei den beaufsichtigten Unternehmen aussehen sollten.

Der BaFin wurden seit 2017 mehr als 400 sogenannte Sicherheitsvorfälle von beaufsichtigten Unternehmen gemeldet. Ein Drittel davon waren mittelschwere bis schwere Vorkommnisse. Meist resultierten diese jedoch nicht aus Cyberangriffen, sondern aus internen Pannen. Nach Ansicht der BaFin setzt die Digitalisierung nicht nur die Geschäftsmodelle unter Druck, sondern bringt auch gewaltige Sicherheitsrisiken mit sich[3]. Und um diese Gefahren kümmerten sich aus Sicht der Aufsicht viele deutsche Geldhäuser zu wenig. Die IT-Systeme seien veraltet, Dienstleister würden nicht ausreichend überwacht und Technologien zu wenig getestet. Hinzu kommt nach Ansicht der BaFin, dass nicht alle Institute genügend Geld investierten, um Cyberangriffe festzustellen und Bedrohungen erkennen zu können, bevor es zu spät ist.

Auch wenn Kapitalverwaltungsgesellschaften keine Banken sind, befassen sie sich gezielt mit der Cybersicherheit, um die Daten ihrer Anleger und Geschäftspartner sowie ihr eigenes Ansehen zu schützen. Dieses Papier soll bei der Formulierung und Umsetzung ihrer Cyber-Sicherheitsstrategie unterstützen.

1. Gefährdungsszenarien in der Fondswirtschaft

Die Fondswirtschaft ist traditionell stark von ihrer Informationstechnik abhängig und damit auch Cyberrisiken ausgesetzt. In den letzten Jahren hat sich die Gefahr von Cybervorfällen verschärft. Dies liegt insbesondere an den technischen Entwicklungen und der stärkeren Vernetzung der Unternehmen, aber auch an der zunehmenden Professionalisierung der Cyberkriminellen. Durch die Angriffe auf Unternehmen und Behörden hat die Sensibilisierung bei den Fondsgesellschaften zugenommen. In der Fondswirtschaft nimmt die Informationsverarbeitung eine herausragende Rolle ein. Fast alle Prozesse werden automatisiert durch Anwendungssysteme umgesetzt oder gesteuert. Für Angreifer, gleich welcher Motivation, stellen die Daten und die Funktionalität der Anwendungen lohnende Ziele dar. Wichtige Angriffsziele sind:

- Handelssysteme und Schnittstellen
- Office- und E-Mail-Systeme
- Unternehmensnetzwerke
- Datenbanken und Dateien
- Buchführende IT-Systeme
- Vorgelagerte Anwendungen
- Steuerungs- und Controlling-Anwendungen
- Anwendungen für Risikomanagement und Risikoberichterstattung
- Schnittstellen zu Anlegern und Geschäftspartnern, z. B. Web-Anwendungen

Cyberkriminalität ist aber mehr als ein Technikproblem; es geht auch um Menschen. So betraf der WannaCry-Angriff 2017 mehr als 230.000 Computer und wurde dadurch erleichtert, dass Mitarbeiter, vor allem von Unternehmen außerhalb der Fondswirtschaft, auf infizierte E-Mails klickten; eine heimtückische Hacking-Technik, die als „Ransomware" bekannt ist.

Was versteht man unter Cybersicherheit?

Cybersicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der klassischen IT-Sicherheit wird dabei auf den gesamten Cyberraum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein.

2. Cybersicherheits-Rechtsrahmen für Kapitalverwaltungsgesellschaften

Kapitalverwaltungsgesellschaften unterliegen als beaufsichtigte Unternehmen bereits hohen Anforderungen an die Sicherheit in der Informations- und Kommunikationstechnik. Mit Blick auf die zentrale Rolle der Informationstechnik gibt die BaFin in den Mindestanforderungen an das Risikomanagement von Kapitalverwaltungsgesellschaften („KAMaRisk") auch Anforderungen an die IT-Prozesse und IT-Systeme vor. Die KAMaRisk verpflichten Kapitalverwaltungsgesellschaften, ihre IT-Systeme und IT-Prozesse zum Schutz der Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität der Daten auf gängige Standards abzustellen.

Zu solchen Standards zählen z. B. der IT-Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der internationale Sicherheitsstandard ISO 27001/27002 der Internationalen Organisation für Normung. Insbesondere werden Benutzerberechtigungsverfahren eingefordert. Kapitalverwaltungsgesellschaften müssen regelmäßig überprüfen, ob ihre IT-Systeme und -Prozesse diese Anforderungen erfüllen. Weiterhin haben sie Software-Entwicklungsprozesse einzurichten. Diese sind ebenfalls sicher auszugestalten. Einen eindeutigen Anforderungskatalog gibt es in den KAMaRisk nicht, vielmehr geht es um „Angemessenheit", wie z. B. den Aufbau einer angemessenen technisch-organisatorischen Ausstattung des IT-Systems oder eines angemessenen Notfallplans.

Die BaFin will die Anforderungen an die IT von Kapitalverwaltungsgesellschaften in einem gesonderten Rundschreiben „KAIT" im Sommer 2019 weiter präzisieren.

Alle Anforderungen gelten unabhängig davon, ob die IT-Systeme und -Prozesse von den Kapitalverwaltungsgesellschaften selbst betrieben werden, ob sie sie ausgelagert haben oder die Leistung auf andere Weise von externen Stellen beziehen. Sie sind notwendig, um eine ordnungsgemäße Geschäftsorganisation sicherzustellen.

Darüber hinaus hat die BaFin ein Merkblatt zur Auslagerungen an Cloud-Anbieter veröffentlicht[4]. Mit dieser Orientierungshilfe teilen die BaFin und die Deutsche Bundesbank ihre gemeinsame Einschätzung zur Auslagerung an Cloud-Anbieter mit. Die Orientierungshilfe verfolgt das Ziel, für die beaufsichtigten Unternehmen ein Problembewusstsein im Umgang mit Cloud-Diensten und den damit verbundenen aufsichtsrechtlichen Anforderungen zu schaffen.

In diesem Zusammenhang weist die Orientierungshilfe auf wesentliche Aspekte hin, die beaufsichtigte Unternehmen bei einer Auslagerung an Cloud-Anbieter z. B. im Rahmen der Risikoanalyse und der vertraglichen Gestaltung beachten sollten.

Als Pflichten kommen nicht nur öffentlich-rechtlich normierte Verhaltensstandards in Betracht, sondern auch und in erster Linie zivilrechtlich begründete Sicherheitspflichten, deren schuldhafte Verletzung zur Haftung des Verantwortlichen führt. Im Rahmen der allgemeinen Sorgfaltspflicht hat die Unternehmensleitung Maßnahmen zur Sicherstellung der Einhaltung gesetzlicher Bestimmungen mittels unternehmensinterner Regeln zu etablieren. Regelverstöße können empfindliche Strafen für ein Unternehmen und seine Organe nach sich ziehen. Daher ist jedes Unternehmen gezwungen, Prozesse und Systeme permanent auf die Einhaltung regulatorischer Anforderungen zu überprüfen. Der Aufbau und die Optimierung eines wirksamen Compliance-Management-Systems gewinnt hierbei immer größere Bedeutung. Ziel ist dabei insbesondere eine Unterstützung der Leitungs- und Aufsichtsorgane bei der Gewährleistung einer ordnungsgemäßen Unternehmensführung und damit die Abwendung von Schäden für die Unternehmung und darüber hinaus die Vermeidung einer persönlichen Haftung von Organmitgliedern (Aufsichtsrat, Vorstand, Geschäftsführung). Als Unterstützung zur Umsetzung und Prüfung gibt es die Normen IDW PS 980 und ISO19600.

Kommt es zu einer Datenschutz-Verletzung, treten unter bestimmten Bedingungen Meldepflichten ein. Wann genau welche Informationspflicht eintritt, regelt die Datenschutz-Grundverordnung (DS-GVO) anders als das bisherige Bundesdatenschutzgesetz (BDSG). Im Vergleich zum BDSG stellt die DS-GVO reduzierte Meldepflichten vor[5]. Demnach müssen sogenannte Datenpannen der Aufsichtsbehörde nicht gemeldet werden, wenn diese voraussichtlich nicht zu einem Risiko für den Betroffenen führen. Die Benachrichtigung an den Betroffenen muss wiederum erst dann erfolgen, wenn ein hohes Risiko für die Rechte und Freiheiten besteht oder wenn Maßnahmen zur Schadensbegrenzung getroffen wurden, die die Möglichkeiten auf ein Risiko beseitigen. Auch die Information gegenüber Betroffenen ist nicht mehr erforderlich, solange technische und organisatorische Maßnahmen vorhanden sind, die einen Zugang zu personenbezogenen Daten unmöglich machen (z. B. Verschlüsselung).

Cyberangriffe zu bemerken und hinreichend schnell auf sie zu reagieren, ist für Kapitalverwaltungsgesellschaften eine Herausforderung. War ein Cyberangriff erfolgreich, so ist es wichtig, dass sie das Ausmaß des Schadens rechtssicher feststellen, um Haftungsrisiken vorzubeugen.

3. Cyber-Sicherheitsarchitektur im Unternehmen

Privatwirtschaftliche Unternehmen außerhalb des Finanzsektors pflegen nicht selten einen reaktiven Ansatz bei Cyber-Bedrohungen und nehmen notwendige Maßnahmen erst dann vor, wenn sie konkret von einem Vorfall betroffen sind. Dies führt im Allgemeinen dazu, dass sie nach dem Verstoß eine Reihe neuer individueller Sicherheitstechnologien und -protokolle „zusammenschustern“, die sich schon beim nächsten Vorfall als weitgehend ineffektiv erweisen können. Vorteilhafter ist ein unternehmensspezifischer Cyber-Sicherheitsrahmen, der Leitlinien bietet, wie ein Unternehmen seine Möglichkeiten zur Prävention, Erkennung und Reaktion auf Cyberangriffe bewerten und verbessern kann.

In diesem Abschnitt betrachten wir einige der wichtigsten Cyber-Sicherheitsthemen, die für den Aufbau einer effektiven Organisation erforderlich sind, und beschreiben die wichtigsten Methoden, die Ihnen helfen können, Ihre Prozesse zu strukturieren.

Um eine gute Cyber-Sicherheitsstrategie zu entwickeln, beachten auch Fondgesellschaften insbesondere die folgenden Aspekte.

Risikoanalyse

Es ist entscheidend, zunächst die aktuelle Gefährdungslage zu analysieren und die künftige Ausrichtung Ihrer Cyber-Sicherheitskontrollen zu definieren. Um sichere Prozesse zu etablieren, müssen Sie die Cyberrisiken kennen, die Sie potenziell bedrohen. Dies bedeutet, dass Sie die in Ihrem Unternehmen vorhandenen Informationen, Daten, IT-Systeme, usw., abbilden und methodisch analysieren müssen, wer sie bedrohen könnte und wie und mit welcher Wahrscheinlichkeit dies erfolgen kann. Hierbei sollten z. B. auch die personenbezogenen Daten der Beschäftigten in die Bewertung der organisatorischen Bedrohungslage einbezogen werden.

Hierzu gibt es eine Reihe von Industriestandards, z. B. den IT-Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und den internationalen Sicherheitsstandard ISO 27001/27002 der Internationalen Organisation für Normung, die Sie verwenden können.

Diese Risiken müssen Sie identifizieren und diese der Risikobehandlung im Unternehmen zuführen.

IT-Governance

Sie sollten Verfahren und Methoden festlegen, wie Cyber-Sicherheitsrisiken in Ihrem Haus verringert werden können, welche Zuständigkeiten bestehen und wie die regelmäßige Berichterstattung an die Leitungsebene erfolgen soll. Die Verantwortlichkeit für angemessene Cyber- Sicherheitsverfahren muss bei der Geschäftsführung liegen, die die Cyber-Sicherheitsstrategie festlegt und deren Fortschritte verfolgt. In Betracht kommt ein Geschäftsführungsmitglied mit Technologieerfahrung oder die Hinzuziehung externer Experten, die das zuständige Mitglied der Geschäftsführung unterstützen können.

Welcher Ansatz auch immer gewählt wird, es muss sichergestellt sein, dass der Verantwortliche in der Leitungsebene das Thema Cybersicherheit ernst nimmt, seine Bedeutung versteht und sich ständig dafür einsetzt, dass sie effizient im Unternehmen betrieben wird. Die Verantwortlichkeit des zuständigen Leitungsmitglieds besteht unbeschadet einer Gesamtverantwortung der Geschäftsführung.

> IT-Governance besteht aus Führung, Organisationsstrukturen und Prozessen, die sicherstellen, dass die Informationstechnik (IT) die Unternehmensstrategie und -ziele unterstützt.
>
> Bundesamt für Sicherheit in der Informationstechnik

Sensibilisierung und Schulung

Das Sprichwort, dass ein Unternehmen nur so gut ist wie seine Mitarbeiter, gilt insbesondere für die Cybersicherheit. IT-Sicherheit ist nur dann möglich, wenn die Mitarbeiter erkennen und akzeptieren, dass sie zum Unternehmenserfolg sowie zur wirkungsvollen IT-Sicherheit beitragen. Deshalb ist es von entscheidender Bedeutung, die Mitarbeiter in allen Bereichen und auf allen Ebenen zu schulen. Es beginnt mit dem Aufbau einer Kultur des Sicherheitsbewusstseins, die „aus der Chefetage“ kommen muss. Grundlegende, gute Verhaltensweisen müssen vermittelt werden, wie z. B. das Nicht-Teilen von Passwörtern oder das Nicht-Klicken auf unbekannte Links. Hierfür sind Richtlinien und Verhaltensregeln festzulegen, die Ihre Mitarbeiter in sicherheitskritischen Situationen anwenden und befolgen müssen.

© photon/fotolia

Der BVI bietet regelmäßig Cybersicherheits-Trainings an. Die Seminare stehen allen Mitarbeitern der Mitglieder offen.
https://events.bvi.de

Das Ziel muss es sein, informierte Nutzer zu schaffen, die sich der Risiken bewusst sind, Klarheit darüber haben, was von ihnen erwartet wird, und über die Instrumente verfügen, die sie dazu benötigen. Es ist wichtig, die Botschaften einfach und leicht verständlich zu halten und sie durch persönliche Lebensbeispiele real und relevant erscheinen zu lassen („Würden Sie Ihr Online-Banking-Passwort mit einem Bekannten teilen?“). Es kann auch sehr wirksam sein, einen Ansatz zu verfolgen, der Mitarbeiter für gutes Verhalten belohnt. Wenn Sie beispielsweise Phishing-Tests intern durchführen, haben Sie möglicherweise eine „Hall of Fame" für Mitarbeiter, die bei der Identifizierung und Meldung von Phishing-E-Mails geholfen haben.

Zusätzlich zu diesen allgemeinen Bildungs- und Sensibilisierungsmaßnahmen können Sie besondere Schulungen für Mitarbeiter anbieten, die mit IT-sensiblen Daten umgehen. Dies betrifft regelmäßig leitende Angestellte, aber auch andere Mitarbeiter in Funktionen, die aufgrund ihrer Aufgaben besonderen Zugang zur IT-gestützten Daten haben, z. B. im Bereich Buchhaltung oder persönliche Assistenten der leitenden Angestellten.

Auch die Kommunikation spielt bei Cyberangriffen eine wichtige Rolle. Ihre Aufgabe ist es, alle Stakeholder inklusive der Presse angemessen und im erforderlichen Umfang über die Datenpanne oder den Angriff zu informieren, um den Reputationsschaden für das Unternehmen so gering wie möglich zu halten. Darauf kann man sich in Musterszenarien vorbereiten, z. B. durch vorbereitende Kommunikation an Kunden, Eigentümer und Öffentlichkeit.

Der BVI erstellt zusammen mit seinen Mitgliedern einen Kommunikationsleitfaden, der die Eckpunkte einer solchen Krisenkommunikation enthält.

Angriffe erkennen, reagieren und Abläufe wieder in Gang bringen

Egal, wie viel Sie in die Cyber-Widerstandsfähigkeit Ihres Unternehmens investieren, Cyberangriffe werden vorkommen. Damit Sie wirkungsvoll auf einen Angriff reagieren und die Prozesse schnell wieder in Gang bringen können, ist von entscheidender Bedeutung, dass Sie einen Angriff als solchen erkennen. Um einen Angriff sicher und rechtzeitig zu erkennen, müssen Sie wissen, welche Netzaktivitäten bei Ihnen normal sind. Dies geschieht durch eine Überwachung der Datenströme über geeignete Messverfahren, z. B. Intrusion Detection Systeme (IDS) und Intrusion Protection Systeme (IPS). Hierdurch ist es möglich, ungewöhnliche Aktivitäten zu erkennen und deren Ursachen zu beseitigen. Darüber hinaus sollten Sie den Anschluss nicht autorisierter Hardware an das Firmennetzwerk mittels geeigneter Systeme überwachen.

Um die Auswirkungen solcher Vorfälle möglichst gering zu halten, sollte Ihr Unternehmen in der Lage sein, möglichst schnell zu reagieren. Hierfür sind klare Verhaltens-Richtlinien für unterschiedliche Formen von Cyberangriffen vorzuhalten. Empfehlenswert sind darüber hinaus regelmäßige Simulationen von Cyber-Sicherheitsereignissen in einem sicheren und kontrollierten Umfeld.

Darüber hinaus werden mittlerweile auf dem Markt spezielle Cyber-Versicherungen angeboten. Die Policen bieten speziellen Versicherungsschutz (z. B. Informationssicherheitsverletzungen, Diebstahl personenbezogener Daten, Internet-Attacken) sowie professionelle Soforthilfe, wie z. B. Zugang zu Cyberforensik-Forschern, spezialisierten Rechtsberatern und PR- und Kommunikationsfachleuten. Hierdurch wird ein Zugang zu Expertenwissen ermöglicht, das innerhalb des eigenen Unternehmens möglicherweise nicht vorhanden ist. Der Umfang des Versicherungsschutzes ist allerdings sehr unterschiedlich und erfordert eine sorgfältige Prüfung, ob Ihre individuellen Bedürfnisse auch tatsächlich abgedeckt sind.

Schlüsselfaktoren

- Der IT- und Cybersicherheit muss zur Realisierung der Chancen und Wachstumspotenziale der Digitalisierung Priorität zukommen.
- Kern eines risikobasierten Vorgehens in Bezug auf den Aufbau einer effektiven Cybersicherheit ist eine Cyber-Sicherheitsstrategie, d. h. die Risikoanalyse und Schaffung interner Sicherungsmaßnahmen.
- Cybersicherheit ist strategische Aufgabe und Teil des Risikomanagements in der Unternehmensführung. Die oberste Leitungsebene muss sich umfassend engagieren, mit Fragen der Cybersicherheit auskennen und klare Verantwortlichkeiten festlegen.
- Entscheider müssen die Prozesse und Strukturen für die IT-Sicherheit unter Einbeziehung aller Abteilungen – von Management über Produktentwicklung bis hin zur IT-Organisation – aktiv vorantreiben.
- Cyber-Sicherheitsrisiken sind laufend zu identifizieren und kategorisieren, um sicherzustellen, dass die getroffenen Sicherheitsmaßnahmen dem Risikopotenzial gerecht werden.
- Die internen Sicherheitsmaßnahmen sind unter Berücksichtigung des Ergebnisses der Risikoanalyse laufend weiterzuentwickeln.
- Mitarbeiter und Dritte müssen über Cyber-Sicherheitsrisiken und den richtigen Umgang mit diesen Risiken aufgeklärt werden.

Beziehungen zu Dritten

Ein wichtiger Teil des Cybersicherheits-Puzzles besteht darin, dass Unternehmen über effektive Prozesse verfügen, die sie in die Lage versetzen, die Cybersicherheit auch bei Einbindung externer Unternehmen sicherzustellen und die Risiken ganzheitlich zu steuern.

Hierzu müssen Sie wissen, mit welchen Unternehmen Ihr Haus zu tun hat, welchen Zugriff diese Unternehmen auf Ihre Daten haben und wie diese Unternehmen mit Ihrem Firmennetzwerk verbunden sind. Stellen Sie sicher, dass die notwendigen Vereinbarungen zur Datensicherheit in bestehenden Verträgen mit diesen Unternehmen enthalten sind, bzw. effektive Prozesse für die Beauftragung externer Unternehmen in Ihrem Haus bestehen. Sie sollten die Zusammenarbeit mit Ihren Vertragspartnern regelmäßig und kontinuierlich auf risikobasierter Basis überprüfen.

Über den Zustand der IT-Sicherheit Ihres Vertragspartners sollten Sie sich idealerweise durch Vorlage einer entsprechenden Zertifizierung vergewissern. In Betracht kommen auch sog. Joint Audits, bei denen sich mehrere Unternehmen zur gemeinsamen Prüfung eines anderen Unternehmens zusammenschließen, um Aufwand und Kosten zu sparen.

4. Cyberrisiko-Plattform für die Fondswirtschaft schaffen

Wie kann die Fondswirtschaft ihre hohen Sicherheitsstandards weiter optimieren? Ein Schlüssel ist sicher eine stärkere Zusammenarbeit.

Cyberrisiko-Informationsaustausch der Fondswirtschaft optimieren

Der BVI setzt sich für einen Cyberrisiko-Informationsaustausch in der Fondswirtschaft ein. Ziel ist die Einrichtung eines speziellen Cyberrisiko-Forums.

Die Plattform könnte allen Branchenteilnehmern aktuelle Informationen zur Bedrohungslage der IT-Sicherheit durch Cyberangriffe, aktuell erkannten Schwachstellen in Software oder Sicherheitslücken von Hardwaresystemen liefern. Der BVI könnte die eingelieferten Daten sammeln und sie in aufbereiteter Form zur Verfügung stellen. Die Fondswirtschaft könnte so Gefahren schneller erkennen und die eigene IT besser schützen. Zudem werden die Nutzer dieser Plattform in die Lage versetzt, die Risiken ganzheitlich zu erfassen, Schwachstellen zu schließen und Hackerangriffe präventiv abzuwehren.

Seit April 2017 ist der BVI Multiplikator der Allianz für Cybersicherheit (ACS) beim Bundesamt für Sicherheit in der Informationstechnik BSI und informiert Mitglieder regelmäßig über die neuesten Hackerangriffe und –strategien, Trojaner und BSI-Aktionen.

Stärkere Zusammenarbeit, um optimale Lösungen zu schaffen

Abhängig von der Größe eines Unternehmens erschweren begrenzte Ressourcen, reduzierte Budgets, steigende Betriebskosten und nicht zuletzt die Komplexität oft die Entwicklung individueller Instrumente zur Minderung von Cyber-Sicherheitsrisiken.

Das in der Fondswirtschaft vorhandene Potenzial kann jedoch nutzbar gemacht werden, wenn die Akteure eng zusammenarbeiten und gemeinsame Ziele verfolgen. Die Fondswirtschaft sollte die Gelegenheit nutzen, gemeinsam an der Entwicklung von Best-in-Class-Lösungen und dem Austausch von Best Practices zu arbeiten, die dann alle Unternehmen nutzen können, z. B. brancheninterne Standards beim internen Reporting oder Security Awareness-Kampagnen für Mitarbeiter.

Cyberangriffe erkennen und reagieren

Unabhängig von der Größe des Unternehmens ist bei einem Cybervorfall sicherzustellen, dass die betroffenen Bereiche innerhalb und außerhalb des Unternehmens rechtzeitig eingebunden werden.

Ähnlich wie beim vorhergehenden Punkt kann die Fondswirtschaft relevante Erkenntnisse austauschen, um Bedrohungen früh genug erkennen und reagieren zu können, Mitarbeiter gemeinsam aus- und fortbilden oder gemeinsam in effektive IT-Lösungen investieren, um Kosten zu sparen. In Betracht kommt schließlich auch die gemeinsame Nutzung von IT-Lösungen oder Fachkompetenz zur Wiederherstellung der IT-Systeme nach einem Notfall oder zur Fortsetzung des Geschäftsbetriebes für die Zeit, in der die eigenen Systeme nicht verfügbar sind.

Auf sachgerechtes Regulierungsniveau achten

Durch eine aktive Festlegung von Mindeststandards kann sich die Fondswirtschaft glaubwürdig in den Regulierungsprozess einbringen und sich für sachgerechte Regeln einsetzen.

Sie wäre in der Lage, den Regulierungsbehörden mit einer einzigen, einheitlichen Stimme wichtige Erkenntnisse und Themen zu vermitteln.

Voneinander Lernen und Erfahrungen austauschen, was funktioniert

Wichtig ist, dass sich die Fondswirtschaft über Techniken austauscht, die sich als erfolgreich erwiesen haben, sowie über die daraus gezogenen Schlüsse, damit andere die Konzepte übernehmen und in ihrem eigenen Unternehmen verwenden können. Ein branchenweites Forum für Cybersicherheit erhöht zudem die Schlagkraft und damit die Einwirkungsmöglichkeiten der Fondswirtschaft auf die relevanten Geschäftspartner. Denn es ist entscheidend, dass die Cyber-Sicherheitsstandards in der gesamten Fondwirtschaft hoch sind, also auch bei IT-Anbietern oder Dienstleistern aus der Finanzbranche, wie Marktdatenanbietern, Börsen oder Verwahrstellen.

Cybersicherheit auch im Anlageuniversum optimieren

Für die Fondswirtschaft ist auch die Cybersicherheit anderer Unternehmen von großer Bedeutung. Eine Studie von Oxford Economics bestätigt, dass Cyberangriffe den Aktienkurs eines Unternehmens beeinflussen können[6]. Die Studie ergab, dass bei 65 Unternehmen, die einen Cyberangriff erlitten hatten, der Vorfall zu einem dauerhaften Rückgang ihres Aktienkurses um knapp 2 Prozent führte. Insgesamt betrug die Abwertung 42 Milliarden US-D.

Es besteht daher ein klarer Anreiz für die Fondswirtschaft, Cybersicherheit auch in anderen Branchen zu fördern. Ein erster Schritt könnte in der Prüfung bestehen, ob Unternehmen, an denen sich die von Kapitalverwaltungsgesellschaften verwalteten Fonds beteiligen, über ein angemessenes Cyber-Sicherheits-management verfügen.

Zusammenfassung

Es ist Zeit, die Zusammenarbeit in der Fondwirtschaft zum Thema Cybersicherheit zu verbessern und neu zu definieren.

Die Fondswirtschaft muss enger zusammenarbeiten und eine Führungsrolle in der Asset-Management-Branche beim Thema Cybersicherheit wahrnehmen.

Folgende Schritte sind zu prüfen:

- Cyberrisiko-Informationsaustausch optimieren
- Cybersicherheits-IT-Standards und deren Umsetzung im Asset Management voranbringen
- Cybersicherheit-Lösungen für Aus- und Weiterbildung und Reporting gemeinsam organisieren
- Abgestimmte Cyber-Abwehrmaßnahmen zwischen Kapitalverwaltungsgesellschaften, Aufsicht und Dienstleistern unterstützen

[1] THE GLOBAL COST OF CYBERCRIME Report Economic impact of cybercrime II Center for Strategic and International Studies June 2014

[2] Handelsblatt vom 20.11.2018: BaFin plant neue „Cyber-Stresstests“ für deutsche Banken

[3] Spiegel-Online vom 22.8.2018: Banken schützen sich nicht gut genug gegen Cyber-Angriffe

[4] https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/BA/dl_181108_orientierungshilfe_zu_auslagerungen_an_cloud_anbieter_ba.html?nn=9021442

[5] Art. 33, 34 DS-GVO

[6] https://www.oxfordeconomics.com/recent-releases/cyber-attacks-effects-on-uk

Herausgegeben von

BVI Bundesverband Investment und Asset Management e.V.

Bockenheimer Anlage 15
60322 Frankfurt am Main

www.bvi.de

Stand: März 2019