SOPHOS

Geschäftsführerhaftung bei Cyber-Angriffen

Cybersecurity und Digital Compliance

Dieser Whitepaper wurde in Zusammenarbeit mit Rechtsanwalt Andreas Daum, LL.M. (LSE) von Noerr Partnerschaftsgesellschaft mbB erstellt.

Sophos-Whitepaper. März 2023

Einleitung

Das Thema IT-Sicherheit wird immer mehr zum Compliance-Thema. Aufgrund der akuten Bedrohung im Cyberraum haben die Europäische Union und ihre Mitgliedstaaten in letzter Zeit immer strengere Vorschriften zur Cybersecurity verabschiedet. Auch die Behörden haben das Thema auf dem Schirm: In Deutschland hat der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg bereits im Jahr 2018 gegen einen Social-Media-Anbieter ein Bußgeld in Höhe von 20.000 Euro verhängt.[1] Zwei Jahre später ordnete die Behörde gegenüber einer gesetzlichen Krankenversicherung sogar ein Bußgeld von über einer Million Euro an.[2] In beiden Fällen verstießen die Adressaten des Bußgelds gegen Vorschriften zur IT- und Datensicherheit. Beispiele lassen sich auch außerhalb der Europäischen Union finden. Im Vereinigten Königreich verhängte das Information Commissioner's Office nach einer verheerenden Cyberattacke gegen ein britisches Luftfahrtunternehmen sogar eine Rekordstrafe in Höhe von 183 Millionen Pfund.[3]

In diesem Paper zeigen wir, inwieweit Cybersecurity auch ein Compliance-Thema ist und wie der MDR-Service von Sophos Unternehmen bei der Bekämpfung von Cyberangriffen unterstützen kann.

1 https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo/, abgerufen am 27.02.2023.
2 https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-bussgeld-gegen-aok-baden-wuerttemberg-wirksamer-datenschutz-erfordert-regelmaessige-kontrolle-und-anpassung/, abgerufen am 27.02.2023.
3 https://www.bbc.com/news/business-48905907, abgerufen am 27.02.2023.

1. Aktuelle Bedrohungslage

Mit dem Beginn des russischen Angriffskriegs gegen die Ukraine hat sich die Lage der IT-Sicherheit in Deutschland nochmals deutlich verschärft. Die oberste Behörde für Cybersicherheit, das Bundesamt für Sicherheit in der Informationstechnik (BSI), bewertet die Bedrohung im Cyberraum so hoch wie nie. Allein im Zeitraum zwischen Juni 2021 und Mai 2022 verzeichnete die Behörde insgesamt 116,6 Millionen neue Schadprogramm-Varianten, 15 Millionen Meldungen zu Schadprogramm-Infektionen und 20.174 Schwachstellen in Software-Produkten. Eine der größten Bedrohungen für die Cybersicherheit von Unternehmen sind Ransomware-Attacken. Dabei verschlüsseln Kriminelle über eine (oftmals per E-Mail aktivierte) Schadsoftware die Daten und Systeme ihrer Opfer und erpressen diese gleich doppelt: Zum einen drohen die Angreifer, die Daten und Systeme nur gegen Lösegeld wieder freizugeben, zum anderen kündigen sie an, geschäftskritische oder personenbezogene Daten zu veröffentlichen, wenn das Opfer nicht sofort zahlt. Im Jahr 2021 wurden nach Angaben des Branchenverbands der deutschen Informations- und Telekommunikationsbranche Bitkom e.V. 84 % der Unternehmen in Deutschland Opfer von Cyber-Angriffen. Dadurch entstand der deutschen Wirtschaft ein Schaden in Höhe von 203 Milliarden Euro. Aus dem Sophos-Ransomware Report 2022[4] geht hervor, dass sich die Höhe der Lösegeldzahlungen gegenüber 2020 vervierfacht hat. Der Schaden eines Cyberangriffs besteht aber nicht (allein) in der Zahlung einer Lösegeldsumme. Vor allem der Produktionsstillstand, der durch solche Attacken möglicherweise ausgelöst wird, kann verheerend sein. Nach dem Sophos-Ransomware Report 2022 braucht es durchschnittlich einen Monat, bis sich die betroffenen Unternehmen von der Attacke wieder erholen. Eine Ransomware-Attacke kostet damit im Durchschnitt 1,4 Millionen Dollar. Aufgrund des langen Bereinigungszeitraums können diese Kosten jedoch noch deutlich höher ausfallen.

Eine künftige Entspannung der Bedrohungslage ist nicht absehbar. Mit der digitalen Transformation und der steigenden Automatisierung und Vernetzung von Systemen und Prozessen bieten sich für Angreifer immer wieder neue Möglichkeiten. Angesichts der dynamischen Bedrohungslage müssen die Unternehmen ihre Cybersecurity-Fähigkeiten daher ständig weiterentwickeln.

4 https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf, abgerufen am 28.02.2023.

2. Compliance-Anforderungen an Geschäftsführung, Vorstand und Aufsichtsrat

Eine funktionierende und sichere IT ist für jedes Unternehmen von elementarer Bedeutung. Ihre Vernachlässigung kann angesichts der erheblichen Bedrohungslage drastische Folgen haben, etwa für die Produktionsprozesse, die Mitarbeiterorganisation oder für Kundenkommunikation und Reputation. Daneben ist auch der Gesetzgeber im Bereich der digitalen Regulierung in den letzten Jahren sehr aktiv gewesen. Mit zahlreichen neuen Gesetzen sowohl auf deutscher als auch europäischer Ebene sind die regulatorischen Anforderungen strenger und komplexer geworden.

Dabei sind Geschäftsführungen, Vorstände und Aufsichtsräte gesetzlich verpflichtet, die IT-Sicherheit ihres Unternehmens sicherzustellen. Bei Pflichtverletzungen drohen hohe Geldbußen für das Unternehmen und die persönliche Haftung von Entscheidungsträgern und Verantwortlichen.

2.1 Pflichten von Geschäftsführung und Vorstand

Aus Compliance-Sicht ist es vor allem Sache der Geschäftsleitung, die Cybersecurity im Unternehmen sicherzustellen. Die gesetzliche Anforderung an die Geschäftsführung einer GmbH und den Vorstand einer Aktiengesellschaft, die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden (§§ 93 Abs. 1 S. 1 AktG, 43 Abs. 1 GmbH), verpflichtet die Verantwortlichen dazu, angemessene Maßnahmen zu treffen, um Gesetzesverstöße und Beeinträchtigungen der IT-Sicherheit zu verhindern.

Die fortschreitende Digitalisierung stellt Unternehmen unter Compliance-Gesichtspunkten vor organisatorische Herausforderungen. Die Geschäftsleitung muss sich fortlaufend über relevante Vorgänge informieren und prüfen, ob Anhaltspunkte für Gefahren für die Cybersecurity oder gar Rechtsverstöße vorliegen. Die Geschäftsleitung muss die jeweiligen Risiken ermitteln und innerhalb des Unternehmens richtig zuordnen. Insgesamt trägt die Geschäftsleitung die Verantwortung für die digitale Infrastruktur des Unternehmens und die Beherrschung der digitalen Risiken. Daher sollten Geschäftsführung und Vorstand ein effektives Risikomanagement einrichten und dieses stetig an die neuen technischen und regulatorischen Entwicklungen sowie die jeweiligen Risikopotenziale anpassen. Dieses Compliance-System umfasst sowohl technische als auch organisatorische Maßnahmen.

Die Pflichten der Geschäftsleitung werden mit der fortschreitenden Digitalisierung weiter an Bedeutung gewinnen. Daher ist die Sicherstellung der Digital Compliance zwingend als oberste Leitungsaufgabe auszugestalten, die von der Geschäftsleitung im Grundsatz als Ganzes wahrzunehmen ist.

2.2 Pflichten des Aufsichtsrats

Die Aufgabe zur Sicherstellung der Digital Compliance trifft auch den Aufsichtsrat, dessen Aufgabe vor allem darin liegt, die wesentlichen Aspekte der Geschäftsleitung zu überwachen (§§ 111 Abs. 1, 76 Abs. 1 AktG). Als zentrale Kontrollinstanz muss der Aufsichtsrat aufpassen, dass die Geschäftsleitung die Risiken digitaler Technologien richtig ermittelt und innerhalb des Unternehmens zutreffend allokiert. Die zunehmende Bedrohungslage für die Vertraulichkeit, Integrität und Verfügbarkeit von Systemen durch Cyberattacken und exponentiell zunehmende Phänomene wie Ransomware haben zur Folge, dass IT-Sicherheitsvorfälle schnell die Existenz eines Unternehmens bedrohen können.

Um den Fortbestand des Unternehmens zu sichern, muss sich der Aufsichtsrat also davon überzeugen, dass im Unternehmen geeignete und angemessene Strukturen zur Sicherstellung der Cybersecurity existieren und deren Funktionsfähigkeit und Effizienz prüfen.

3. Haftung

Bei Cyberangriffen oder Verstößen gegen IT-Sicherheits-rechtliche Vorschriften drohen der Geschäftsführung, dem Vorstand und/oder den Aufsichtsratsmitgliedern rechtliche Nachteile.

Die Geschäftsleitung oder Aufsichtsratsmitglieder können zivilrechtlich auf Schadensersatz haften, wenn sie ihre Pflichten zur Sicherstellung der Digital Compliance vorsätzlich oder fahrlässig verletzen. Darüber hinaus können die Mitglieder der Geschäftsleitung und des Aufsichtsrats auch strafrechtlich haften. Ein solcher Fall wäre denkbar, wenn aufgrund vorsätzlichen oder fahrlässigen Verhaltens durch einen Cybervorfall Geschäftsgeheimnisse oder Know-how des Unternehmens gegenüber unbefugten Dritten offenbart werden würden oder ein Angriff dazu führen würde, dass das Unternehmen seinen Geschäftsbetrieb vollständig einstellen muss und dadurch in die Insolvenz schlittert.

Dem Unternehmen selbst können ebenfalls erhebliche Geldbußen drohen. Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), das vor allem die Betreiber „Kritischer Infrastrukturen", die Anbieter „Digitaler Dienste" und „Unternehmen im besonderen öffentlichen Interesse" betrifft, sieht Geldbußen in Höhe von bis zu 20 Millionen Euro vor. Nach der kürzlich verabschiedeten Richtlinie NIS 2.0 wird sich dieser Rahmen künftig weiter verschärfen. Die Richtlinie sieht Sanktionen in Höhe von 2 % des weltweiten Jahresumsatzes vor. Noch drastischer können sich Verstöße gegen die datenschutzrechtlichen Vorschriften auswirken. Hier drohen Geldbußen von bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes.

4. Risikomanagement und Cyberversicherung

Ein wesentlicher Bestandteil einer ordnungsgemäßen Compliance-Organisation ist die Implementierung eines Risikomanagement-Systems. Eine Cyberversicherung kann dabei unterstützen, das Risiko einer wirtschaftlichen oder finanziellen Beeinträchtigung durch Cybervorfälle zu minimieren.

Indes entbindet eine Cyberversicherung die Unternehmen nicht von ihren gesetzlichen Pflichten zur Sicherstellung der IT-Sicherheit. Zudem greift der Versicherungsschutz in der Regel nicht bei vorsätzlichem oder grob fahrlässigem Verhalten. Eine Cyberversicherung kann also immer nur eine flankierende Maßnahme im Risikomanagement des Unternehmens sein, das aus technischen und organisatorischen Maßnahmen nach dem Stand der Technik besteht. Darunter fallen insbesondere Sicherungsmaßnahmen an den Endpoints eines Netzwerks, im Netzwerk selbst und im Bereich E-Mail sowie die Erfassung und Auswertung verdächtiger Ereignisse. Die Geschäftsleitung muss sich der digitalen Risiken im Unternehmen bewusst sein und eventuelle Lücken so gut wie möglich schließen.

Darüber hinaus dürften Qualität, Kosten und Umfang einer Cyberversicherung unter anderem davon abhängen, wie das Versicherungsunternehmen die Wahrscheinlichkeit einer Realisierung digitaler Risiken beim Versicherungsnehmer beurteilt. Kann die Geschäftsleitung nachweisen, dass sie die IT-Sicherheit im Unternehmen gut aufgestellt hat, wird sich dieser Umstand in der Verhandlung mit dem Versicherer positiv auf den Versicherungsschutz und die Versicherungsprämien auswirken.

5. Risikomanagement – Technik ist nicht genug

Bei ihrem Risikomanagement dürfen die Verantwortlichen nicht allein auf technische Maßnahmen setzen, sondern müssen menschliche Expertise miteinbinden. Denn viele Angriffe, bei denen sich die Hacker durch gestohlene Informationen Zugriff auf die Daten und Systemen ihrer Opfer verschaffen, verlaufen still und heimlich. Die Unternehmen stehen vor der Herausforderung, diese Angriffe bereits in der Entstehungsphase zu stoppen, noch bevor ein Schaden entstehen kann. Hierzu sind spezialisierte Bedrohungsexperten notwendig, die auf dem Arbeitsmarkt nur schwer zu finden sind und oft teuer eingekauft werden müssen. Deshalb entscheiden sich viele Unternehmen für einen MDR-Service (Managed Detection and Response), der die eigene IT-Abteilung bei der Aufdeckung und Bekämpfung von Cyberangriffen unterstützt. Bis zum Jahr 2025 werden laut dem Analysten Gartner 50 % aller Betriebe einen MDR-Service nutzen.

6. Unterstützung bei der Digital Compliance durch den Sophos MDR-Service

Der branchenführende MDR-Service von Sophos kann beim Umgang mit der Bedrohungslage und der Einhaltung komplexer regulatorischer Anforderungen in der IT-Sicherheit unterstützen. Die externe Unterstützung bei der Abwehr von Cyberangriffen ist damit ein wichtiger Baustein beim Management digitaler Risiken und hilft den Verantwortlichen, ihre gesetzlichen Pflichten zu erfüllen.

6.1 Was leistet ein MDR-Service genau?

Um nachzuvollziehen, welche Vorteile der MDR-Service von Sophos bietet und was sich hinter der wachsenden Nachfrage nach MDR-Services verbirgt, ist es wichtig zu verstehen, was ein MDR-Service eigentlich ist – und was nicht. Managed Detection and Response (MDR) ist ein 24/7 Fully-Managed Service durch ein Team von Sicherheitsexperten, das darauf spezialisiert ist, Cyberangriffe zu erkennen und zu bekämpfen, die Technologie-Lösungen alleine nicht verhindern können. Die tägliche Cybersecurity-Verwaltung, wie die Bereitstellung von Sicherheitstechnologien, die Aktualisierung von Richtlinien oder die Installation von Updates, sind dagegen nicht Teil des MDR-Services. Managed Service Provider (MSPs) bieten entsprechende IT Security Management Services für Unternehmen und Einrichtungen, die Unterstützung in diesem Bereich benötigen.

Dem MDR-Service von Sophos, der Kunden bei der Abwehr von hochkomplexen Bedrohungen wie Ransomware-Attacken umfangreich unterstützt, vertrauen weltweit über 15.000[5] Unternehmen und Einrichtungen. Mit Bestnoten von Gartner Peer Insights™[6] und der Auszeichnung als „Top Vendor" im Grid® 2022 von G2 für MDR-Services im Midmarket-Segment[7] ist die Cyber-Abwehr bei Sophos in den besten Händen.

5 https://www.sophos.com/de-de/products/managed-detection-and-response, abgerufen am 27.02.2023.
6 https://www.sophos.com/de-de/products/managed-detection-and-response, abgerufen am 27.02.2023
7 https://www.sophos.com/de-de/products/managed-detection-and-response, abgerufen am 27.02.2023.

6.2 Varianten von MDR-Services

Viele Unternehmen und Einrichtungen aus verschiedenen Branchen nutzen bereits einen MDR-Service – von kleinen Unternehmen mit begrenzten IT-Ressourcen bis hin zu Großkonzernen mit eigenem Security Operations Center (SOC). Viele Verantwortliche haben also bereits erkannt, dass für die digitale Compliance des Unternehmens die interne IT-Abteilung mit zusätzlicher Expertise von außen unterstützt werden muss, um alle gesetzlichen Vorgaben einzuhalten und das Haftungsrisiko zu minimieren. Aber wie genau funktioniert hier die Zusammenarbeit zwischen Unternehmen und Dienstleister? Es gibt drei wesentliche Modelle von MDR-Services:

- Das MDR-Team verwaltet die Reaktion auf Bedrohungen komplett für den Kunden
- Das MDR-Team arbeitet mit dem IT-Team des Kunden zusammen und koordiniert gemeinsam die Reaktionsmaßnahmen
- Das MDR-Team benachrichtigt das IT-Team des Kunden und gibt Hilfestellung bei der Behebung von Störungen

Sophos unterstützt alle drei Modelle und passt diese bei Bedarf an die spezifischen Kundenanforderungen an. Der MDR-Service von Sophos kann das Risikomanagement der Verantwortlichen individuell und zielgenau ergänzen und dabei unterstützen, den gesetzlichen Pflichten zur Implementierung angemessener Cybersecurity-Maßnahmen nachzukommen.

6.3 Die 6 wichtigsten Vorteile des MDR-Service von Sophos

Der MDR-Service hilft den Verantwortlichen bei der Digital Compliance wie folgt:

6.3.1 Verbesserung der Cyber-Abwehr

Einer der Hauptvorteile des MDR-Services von Sophos gegenüber unternehmenseigenen Security-Operations-Programmen liegt in dem erhöhten Schutz vor Ransomware und anderen komplexen Cyberbedrohungen. Die Kunden profitieren vom weitreichenden Erfahrungsschatz der Analysten, die sich im Gegensatz zum einzelnen Unternehmen fortlaufend mit verschiedensten Angriffen befassen. So verfügen die Analysten über weitreichende Kenntnisse, die sich interne IT-Teams in dieser Tiefe kaum aneignen können. Die MDR-Teams von Sophos untersuchen täglich viele Vorfälle und reagieren permanent auf Bedrohungen, so dass sie über viel Routine bei der Bedrohungserkennung und -abwehr verfügen. So können die Experten in allen Phasen des Prozesses schneller und genauer reagieren – vom Erkennen wichtiger Signale bis hin zum Analysieren potenzieller Vorfälle und dem Stoppen schädlicher Aktivitäten. Darüber hinaus unterstützt Sophos seine Kunden dabei, nach einem vereitelten Angriff diesen genauer zu analysieren, inklusive Infektions- und Verbreitungswege im Unternehmen. Auf diese Weise können Schwachstellen in der IT-Infrastruktur identifiziert werden, die dann basierend auf Empfehlungen der Sophos-Experten geschlossen werden können.

6.3.2 Mehr Zeit in der IT-Abteilung für andere Aufgaben

Das Threat Hunting, also die Suche nach Bedrohungen im Cyberraum ist zeitaufwändig und unvorhersehbar. IT-Experten, die mit mehreren Aufgaben und Prioritäten jonglieren, können dabei verständlicherweise nicht jeder Spur nachgehen: 79 % der IT-Abteilungen räumen ein, dass sie nicht in der Lage sind, alle Protokolle vollständig zu prüfen, um verdächtige Signale und Aktivitäten zu erkennen[5]. Angesichts der potenziellen Auswirkungen eines Angriffs sollten IT-Teams jedoch sofort alles stehen und liegen lassen, wenn verdächtige Aktivitäten beobachtet werden, um die Bedrohung zu analysieren und umgehend zu bekämpfen. Die Dringlichkeit der Arbeit führt meist dazu, dass sich die internen IT-Teams nicht mehr auf strategisch wichtige – und oft interessantere – Projekte konzentrieren können. Die Zusammenarbeit mit dem MDR-Service von Sophos ermöglicht, Kapazitäten in IT-Teams freizusetzen, um damit für den Geschäftserfolg wesentliche Aufgaben voranzutreiben. Unternehmen, die den MDR-Service von Sophos nutzen, berichten immer wieder von erheblichen Effizienzsteigerungen in ihrer IT, wodurch sie wiederum ihre Unternehmensziele besser erreichen können.

6.3.3 Zuverlässige 24/7-Sicherheit

Da Angreifer rund um den Globus verteilt sind, können sie zu jeder Tages- und Nachtzeit zuschlagen. Angreifer sind besonders dann aktiv, wenn die IT-Abteilung offline ist, z. B. abends, an Wochenenden oder an Feiertagen. Bedrohungserkennung und -reaktion sind demzufolge eine 24-Stunden-Aufgabe und jedes Unternehmen, das diese Aktivitäten auf Bürozeiten beschränkt, geht ein hohes Risiko ein. Der MDR-Service von Sophos bietet einen 24/7-Schutz und sorgt so für die Gewissheit, dass zu jedem Zeitpunkt für Sicherheit gesorgt ist. Für IT-Abteilungen bedeutet dieser Service buchstäblich, nachts besser schlafen zu können. Für Führungskräfte und Kunden bieten routinierte 24/7-Experten mit umfangreichen Praxiswissen über aktuelle Cyberangriffe die Gewissheit, dass ihre Daten und das Unternehmen selbst gut geschützt sind. Damit kann der MDR-Service von Sophos einen wichtigen Beitrag zur Einhaltung der gesetzlichen Vorgaben leisten und das Haftungsrisiko für das Unternehmen und seine Verantwortlichen senken.

6.3.4 Mehr Expertise ohne mehr Personal

Die Erkennung und Abwehr von Cyberangriffen ist ein sehr komplexer Vorgang. Für diese Tätigkeit werden hochspezialisierte Bedrohungsexperten benötigt. Diese müssen über ein breites Spektrum an Fähigkeiten verfügen, darunter Datenanalyse, Programmieren, aktive Bedrohungssuche etc. Außerdem müssen sie umfassende Kenntnisse über Angriffs-Strategien und Schadsoftware besitzen. In jeder dieser Disziplinen sind tagesaktuelles Wissen und stetige Fortbildungen obligatorisch. Leider ist diese Kombination von Kompetenzen rar gesät, sodass es für viele Unternehmen schwierig – wenn nicht fast unmöglich – ist, entsprechend qualifizierte Sicherheitsexperten anzuwerben. Der Aufbau eines entsprechenden Teams, das 24/7 an 365 Tagen im Einsatz ist, kostet schnell mehrere Millionen.

Der MDR-Service von Sophos liefert dieses Know-how als Service-Leistung. Bei Sophos arbeiten hunderte von erfahrenen Analysten, Bedrohungsexperten und Programmierern, die Kunden auf der ganzen Welt schützen. Weiterhin verfügen die Sophos MDR-Experten über tagesaktuelles Bedrohungswissen – dank eines globalen Austauschs über neue Angriffstechniken und aktuelle Vorfälle. Neue Erkenntnisse über Sicherheitslücken und Cyber-Angriffe werden „just in time" global ausgerollt und im Rahmen der Bedrohungssuche genutzt.

Mit Sophos MDR können Unternehmen ihre Security Operations ohne zusätzliches Personal einfach und schnell aufstocken und von tagesaktuellem Wissen profitieren. Dadurch ist Sophos MDR meistens wirtschaftlicher und effizienter als ein internes IT-Security-Team.

6.3.5 Verbesserung des Return on Investment in der Cybersecurity

Ein 24/7 verfügbares Team von Threat Huntern, Analysten und Incident Respondern ist teuer. Um eine 24-Stunden-Abwehr zu gewährleisten, benötigen die Unternehmen in der Regel mindestens fünf oder sechs Cybersecurity-Mitarbeiter (pro Funktion), die in separaten Schichten arbeiten. Durch die Nutzung von Skaleneffekten ist der MDR-Service von Sophos im Vergleich wesentlich günstiger, sodass Unternehmen mehr aus ihrem Cybersecurity-Budget herausholen können. Das Investment in die Cybersecurity lohnt sich fast immer, weil der Schaden eines erfolgreichen Cyberangriffs in der Regel um ein Vielfaches höher ausfällt als die Kosten der Sicherheitsmaßnahmen. Hinzu kommt, dass – wie eingangs bereits erläutert – Cybersecurity mittlerweile auch ein Compliance-Thema ist. Neben Produktionsstillstand und Bereinigung bzw. Neuaufbau der IT kann es auch zu Bußgeldern und einer Haftung von Geschäftsführung und Vorstand kommen. Wenn man berücksichtigt, dass die Behebung eines Ransomware-Angriffs durchschnittlich 1,4 Millionen US-Dollar kostet (Sophos Ransomware-Report 2022), erscheinen die Investitionen in Präventionsmaßnahmen verhältnismäßig gering.

6.3.6 Bessere Chancen auf eine gute Cyberversicherung

Um eine gute Cyberversicherung abzuschließen, müssen Unternehmen häufig nachweisen, dass sie moderne Schutztechnologien zur Abwehr von Cyberangriffen einsetzen. Hierzu zählen in der Regel eine Next-Gen Endpoint Protection sowie Endpoint oder Extended Detection and Response (EDR/XDR). Der Sophos MDR-Service beinhaltet sowohl die erforderlichen Next-Gen-Technologien Endpoint Protection und XDR als auch die spezialisierten Experten, die diese Technologien fachkundig bedienen. Der MDR-Service von Sophos kann damit das Risikomanagement gleich in doppelter Hinsicht unterstützen: Erstens durch die bestmögliche Abwehr von Schäden durch Cyber-Angriffe und zweitens durch die Chance auf einen guten Versicherungsschutz. Dadurch sinkt bei den Verantwortlichen die Gefahr, für unzureichendes Risikomanagement in die Haftung genommen zu werden.

Fazit

Die Komplexität und Zahl der Angriffe im Cyberraum ist in der Vergangenheit stetig gestiegen. Aufgrund der erhöhten Bedrohungslage haben auch die regulatorischen Anforderungen an Unternehmen und Einrichtungen zugenommen. Das deutsche IT-Sicherheitsgesetz 2.0 und die europäische Richtlinie NIS 2.0 haben die gesetzlichen Pflichten noch einmal erweitert und verschärft. In der Folge wird es für Unternehmen und Einrichtungen kaum mehr möglich sein, sich allein auf technische Maßnahmen zu verlassen. Vielmehr sind sie gefordert, auch menschliche Expertise in ihre Cybersecurity-Organisation miteinzubinden. Andernfalls können die Defizite in der Cybersicherheit auch für Geschäftsführung und Vorstand ein Haftungsrisiko darstellen. Die beste Gelegenheit, auf diese Expertise schnell und unkompliziert zurückzugreifen, ist der MDR-Service von Sophos. Die Sophos-Experten sind rund um die Uhr im Einsatz, so dass Sie auch bei den schlimmsten Virusvarianten gelassen bleiben und sich voll auf Ihr Kerngeschäft konzentrieren können.

Weitere Informationen zum Sophos MDR-Service erhalten Sie unter sophos.de/mdr

Sophos bietet branchenführende Cybersecurity-Lösungen für Unternehmen jeder Größe und schützt Kunden in Echtzeit vor komplexen Bedrohungen, wie Malware, Ransomware und Phishing. Bewährte Next-Gen-Funktionen mit der Power von Machine Learning und künstlicher Intelligenz sichern Unternehmensdaten effektiv.

2023-03-22 (WP-NP)

SOPHOS