LINK11

IT-Sicherheit ist mehr als Technik

DIE ROLLE DES CISO RÜCKT IN DEN FOKUS

www.link11.com

Die Rolle des CISO rückt in den Fokus

Die Digitalisierung verspricht der Wirtschaft neue Möglichkeiten. Geschäftsführer und Vorstände der Unternehmen entscheiden jetzt, wohin sich das Geschäft entwickeln soll und wie die Wertschöpfungsketten von morgen aussehen werden. Für die Zukunftsfähigkeit setzen sie auf neue Technologien, Automatisierung und eine intelligente Produktion. Mit fortschreitender Digitalisierung hängt der Unternehmenswert aber zunehmend von neuen Geschäftsmodellen ab, die auf immateriellen Vermögensgegenständen fußen, so wie Daten, Plattformen und Softwareanwendungen. Die Verfügbarkeit, Integrität und IT-Sicherheit von Diensten und Daten werden zur Grundbedingung, um das Tagesgeschäft überhaupt betreiben zu können.

Organisationsformen und Rollenverteilungen sehen sich mit ändernden Marktbedingungen und -anforderungen konfrontiert und gehören daher auf den Prüfstand.

Sichere Umsetzung des digitalen Wandels

Für eine im wahrsten Sinne des Wortes sichere Planung und Umsetzung des digitalen Wandels müssen viele Herausforderungen gemeistert werden: Eine der wichtigsten besteht in der Anpassung der internen Organisationsformen und der Neuverteilung von Rollen im Risikomanagement. Rund die Hälfte der deutschen Unternehmen ist von Cyber-Kriminalität betroffen, stellt die Unternehmensberatung Rochus Mummert in einer Umfrage unter deutschen Unternehmen von Anfang des Jahres 2019 fest.[1] Beim digitalen Wandel zählen deshalb neben Investitionen die Schaffung neuer Strukturen und Rollen, um Geschäftsrisiken zu lindern und abzuwenden.

Bei der Restrukturierung der Organisationsformen sollten Geschäftsführungen und Vorstände den digitalen Wandel zur Chefsache machen. Darüber hinaus müssen die Verantwortlichen für Digitalisierung und IT-Sicherheit bei strategischen und Geschäftsentscheidungen von Anfang an in die Planung miteinbezogen werden.

„Letzten Endes führt die Fortentwicklung von Geschäftsmodellen und Wertschöpfungsketten immer auch zu der Notwendigkeit einer Neubewertung der internen Organisationsstruktur, um den vorhandenen und u. U. neu hinzugekommenen Haftungsrisiken besser Rechnung tragen zu können“, erklärt Professor Dr. Thomas Grützner, Partner bei Latham & Watkins und spezialisiert auf Compliance- und Wirtschaftsstrafrechtsfragen. „Das kann bei immateriellen Vermögensgegenständen oft komplexer sein als bei materiellen, insbesondere, wenn sich aus den bisherigen Geschäftsmodellen keine vergleichbaren Erfahrungswerte oder auch Risiken herausgebildet haben.“

88%

der Unternehmen sind sich bereits darüber im Klaren, dass mit der Digitalisierung ihre Angriffsfläche für Bedrohungen aus dem Cyber-Raum wächst BSI

Neun von zehn Unternehmen in Deutschland sind sich bewusst, dass sie der digitale Wandel angreifbarer macht.[2] Auch darüber, dass Cyber-Bedrohungen eine relevante Bedrohung für die Betriebsfähigkeit darstellen, herrscht mit 76 % der Antworten Konsens. Es vergeht keine Woche, in der Unternehmen die Öffentlichkeit nicht über Sicherheits-Vorfälle und Datenpannen informieren. Die Schlagzeilen und Schadensmeldungen zeigen, wie konkret die Existenzbedrohung durch Unterbrechung von Betriebsabläufen, Ausfall von Diensten sowie Verlust oder Manipulation von Daten sein kann. „Damit geht regelmäßig die Frage nach der internen Verantwortlichkeit wie auch der externen (zivilrechtlichen oder strafrechtlichen) Haftung einher. Unternehmen haben mit diesen veränderten Rahmenbedingungen zu kämpfen und lernen oft erst aus schmerzhaften eigenen Erfahrungen", so Thomas Grützner. Das belegen Vorfälle der vergangenen Monate:

Anfang März kämpfte ein Energieunternehmen, das mehrere westliche US-Bundesstaaten mit Strom versorgt, wegen DDoS-Attacken zehn Stunden lang mit „Unterbrechungen beim Betrieb elektrischer Anlagen".[3]

Im März 2019 mussten beim norwegischen Aluminiumhersteller Norsk Hydro weltweit alle Produktions- und Verwaltungsabläufe gestoppt werden, weil sich Ransomware im Firmennetzwerk ausgebreitet hatte.

Ebenfalls im März 2019 häuften sich bei der Kriminalpolizei in Kempten (Allgäu) Anzeigen, da bei zahlreichen Unternehmen in erpresserischer Absicht Daten und Festplatten verschlüsselt worden waren. Zu den Opfern zählten Firmen, Arztpraxen und Autohäuser.

IT-Sicherheit ist eine Vollzeitaufgabe

Dennoch ist es erstaunlich, dass bis heute zu wenige Firmen das Thema IT-Sicherheit im Top-Management verankern und Cyber-Risiken intern mit Top-Priorität angehen. Die „Global Information Security Survey 2018–19" von EY stellt fest, dass mit 45 % immer noch zu wenige Unternehmen die IT-Sicherheit bereits fest in ihre Geschäftsstrategie integriert haben.[4] In 60 % der Unternehmen gehört der Verantwortliche für IT-Sicherheit nicht dem Vorstand an.[5] Unternehmen benötigen jedoch entsprechende Führung und Prozesse, um ihre digitale Transformation durch geeignete Sicherheitsmaßnahmen professionell zu begleiten. Dieses Aufgabenfeld wird zunehmend an der Position des Chief Information Security Officers (CISO) festgemacht. Der CISO soll Informationsrisiken identifizieren, kommunizieren und managen. Letzteres Handlungsfeld geht über den reinen technischen Bereich hinaus und erstreckt sich bis in die Rechtsabteilung und die Führungsebene.

55%

der Unternehmen sehen Sicherheit immer noch nicht als Teil der Unternehmensstrategie EY

Das Aufgabengebiet eines CISOs gestaltet sich sehr dynamisch. Kerntätigkeiten seiner Arbeit sind die folgenden:

- Strategische Planung und Entwicklung von Konzepten und Richtlinien für die IT-Sicherheit. Dabei arbeitet er eng mit allen Fachabteilungen und mit Partnern zusammen. Verantwortung für die technische Implementierung
- Steuerung und Koordination von Sicherheitsmaßnahmen
- Kontinuierliche Analyse und Optimierung der IT-Sicherheitsstrategien unter Berücksichtigung der Geschäftsprozesse
- Übernahme von Aufgaben aus dem Bereich Prävention, also Entwicklung von Schulungsmaßnahmen zur Sensibilisierung von Mitarbeitern

Gemäß dem Report „Global State of Information Security Survey 2018" von PWC[6] haben bereits 52 % der global befragten Unternehmen die zentrale Position des CISO geschaffen und demnach die Bedeutung des Themas „Sicherheit" für ihre Organisation erkannt. Im Jahr 2006 lag der entsprechende Wert noch bei 22 %.[7] In Deutschland liegt bei 36 % der Unternehmen die Verantwortung für die IT-Sicherheitsstrategie in den Händen eines CISOs.[8] „Diese Entwicklung wird mit der zunehmenden Bedeutung von immateriellen Vermögensgegenständen eines Unternehmens und damit korrespondierend mit den steigenden Haftungsrisiken bei mangelhafter IT-Sicherheit voranschreiten", erläutert Thomas Grützner und fährt fort: „Es ist zu erwarten, dass der Gesetzgeber und die Rechtsprechung hier weiter tätig werden und die gesetzlichen Rahmenbedingungen wie auch die Haftungsmaßstäbe an die zunehmende Bedeutung von immateriellen Vermögensgegenständen anpassen und konkretisieren. Die DSGVO ist ein Schritt in diese Richtung, das diskutierte Unternehmenssanktionenrecht wäre für Straftaten aus dem Unternehmen heraus ein weiterer."

Alternativ übernehmen der Chief Information Officer/CIO (27 %) und das Senior Management die Absicherung von Kommunikation, Technologien und Daten im Unternehmen. Generell gilt: Je größer das Unternehmen ist, desto eher wird das Thema IT-Sicherheit an Spezialisten wie einen CISO übertragen.[9] In den Händen des CEOs, also tatsächlich als Chefsache eingestuft, liegt die Informationssicherheit nur in Ausnahmefällen und auch nur in sehr kleinen Unternehmen. Die Verantwortung für IT-Sicherheit ist vorrangig im Senior Level angesiedelt, fasst die Global Information Security Survey 2018-2019 von Ernst & Young zusammen.[10]

52%

der Unternehmen geben an, dass sie einen CISO ernannt haben PWC

Mehr Nähe des CISOs zum Top-Management

In der analogen Welt spielte die IT in zahlreichen Unternehmen eine rein unterstützende Rolle. Mit der Digitalisierung rückt sie nun in den Kern des unternehmerischen Handelns. Störungen, Betriebsunterbrechungen und Datenpannen beeinflussen unmittelbar das operative Geschäft und dadurch die Finanzkennzahlen. Nahezu sämtliche Entscheidungen in der Industrie 4.0 betreffen die IT der Unternehmen und besitzen daher Relevanz für die Arbeit des CISOs. Es ist dessen Aufgabe, neue Risiken zu erkennen, zu bewerten und möglichst zu mildern oder optimalerweise abzuwenden.

Ob Einführung neuer Produkte oder Übernahme von Unternehmen (M&A) - die Verantwortlichkeiten des CISOs reichen weit über die Auswahl von Firewalls und Virenscannern oder ein systematisches Patchmanagement hinaus. Neben technischen Fähigkeiten muss er zunehmend unternehmensorientiert denken, etwa bei der Bewertung von Risiken beim Kauf immaterieller Vermögensgegenstände wie Software oder Daten. Wenn ein DAX-Konzern ein innovatives Start-up übernimmt, gehen neben dem eingekauften Know-how auch die Haftungsrisiken des Start-ups auf den Konzern über. Versäumnisse aus der Vergangenheit des übernommenen Unternehmens, etwa vorhandene Sicherheitslücken, können den Konzern als neuen Eigentümer überraschend einholen. Bußgelder bei einer Datenpanne, die laut DSGVO bis zu 4 % des Jahresumsatzes betragen können, erreichen bei einem Start-up niedrigere Beträge, als wenn der Jahresumsatz des neuen Eigentümers, des Konzerns, als Bemessungsgrundlage herangezogen wird. Wie wichtig die Verfügbarkeit eines CISOs bei der Übernahme von Unternehmen sein kann, zeigen Zahlen aus dem Gesundheitssektor. Die Beratungsfirma West Monroe Partners hatte Manager, die auf das Abschließen von Kaufverträgen im Bereich Healthcare spezialisiert sind, zu deren Strategien und Erfahrungen befragt. 58 % der Befragten gaben an, dass nach Abschluss der Übernahme ein Problem im Bereich der IT-Sicherheit bei dem erworbenen Unternehmen festgestellt worden war.[11]

58%

der Käufer eines Unternehmens aus dem Gesundheitssektor entdeckten nach Abschluss der Transaktion ein IT-Sicherheitsproblem bei dem erworbenen Unternehmen West Monroe Partners

Direkte Berichtslinie zur Unternehmensleitung

Die Position des CISOs, die es seit den 1990-er Jahren gibt, führte lange ein Schattendasein. Bislang existiert noch kein Standard, der das Aufgabenfeld dieser Position und die damit verbundenen Berichtswege im Unternehmen definiert. Typischerweise berichtet ein CISO noch an den CIO und damit nur indirekt an den Vorstand. Eine solche hierarchische Eingliederung kann überdies zu Interessenskonflikten führen, da in diesem Fall Entwicklung und Betrieb der IT nicht von IT-Sicherheitsfragen getrennt sind. Grützner macht darauf aufmerksam, dass ein Unternehmen sich auch die Frage stellen kann, ob die Berichtslinien den Organisations- und Aufsichtspflichten im Unternehmen in jedem Fall gerecht werden.

Darüber hinaus kann der CISO in das Spannungsfeld zwischen CIO und Chief Financial Officer (CFO) geraten. Der Verantwortungsbereich des CFO weitet sich zunehmend auf Bereiche wie Digitalisierung und IT-Sicherheit aus. Damit kontrolliert der CFO auch die IT-Budgets. Die IT-Sicherheit wird in dieser Konstellation aber nicht immer als Teil der unternehmerischen Wertschöpfungskette gesehen. Vorausschauende, kostenintensive Investitionen in die Sicherheit von IT-Infrastrukturen, Daten und Geräten sind aus dem Blickwinkel der Effizienzsteigerung nur schwer zu vermitteln. Hier ist ein Umdenken gefragt, das IT-Sicherheit nicht als reinen Kostenfaktor identifiziert, sondern als Differenzierungsfaktor gegenüber anderen Anbietern und als Wegbereiter des digitalen Wandels aufwertet. Angesichts eines immer intensiveren Wettbewerbs kann ein Unternehmen über sichere digitale Prozesse Vertrauen im Markt aufbauen und sich über dieses Merkmal von anderen Anbietern abheben. Diese Chance haben aktuell erst 29 % der Unternehmen erkannt. Gleichzeitig hilft IT-Sicherheit, finanzielle Risiken zu minimieren. Schadenssummen, die durch Cyber-Attacken entstehen, können Investitionen in die Sicherheit von Infrastrukturen und IT-Landschaften schnell um ein Vielfaches übersteigen.

Eine direkte Berichtslinie zum Vorstand bedeutet aber per se noch nicht, dass IT-Sicherheit tatsächlich die erforderliche Priorität im Unternehmen besitzt. Jedes Unternehmen muss für sich selbst eine Form der Unternehmensorganisation finden, in der die Einwände des Verantwortlichen für IT- und Informationssicherheit in den vorhandenen Strukturen ausreichend weiterverarbeitet werden können. „Letzten Endes wird die konkrete Ausgestaltung der Governance-Strukturen auch das Ergebnis einer Risikoanalyse des kompletten Unternehmens sein müssen“, prognostiziert Grützner. Grundsätzlich wird eine enge Zusammenarbeit mit dem CEO in Fragen der IT-Sicherheit ein guter Weg sein. Auch die Berichtslinie CISO – Chief Compliance Officer (CCO) – CEO kann ein Gleichgewicht zwischen dem CIO, der den digitalen Wandel maßgeblich vorantreibt, und dem CISO, der in IT-Sicherheitsfragen Vorsicht walten lässt, schaffen.

Direkte Berichtswege des CISOs an den Vorstand werden als Indikator dafür gesehen, dass die IT bzw. IT-Sicherheit intern als unternehmenskritisch bewertet wird. Auf den hohen Stellenwert der Position zahlt ebenfalls ein, wenn IT-Sicherheit, repräsentiert durch den CISO, bei wichtigen Projekten bereits in die strategischen Projektanforderungen und nicht erst bei

29%

der Unternehmen sehen Cyber-Sicherheit als Innovationstreiber, mit dem sie sich vom Wettbewerb abheben können BSI

konkreten Umsetzungsfragen im Rahmen des laufenden Projekts eingebunden wird. Durch konsequente Kommunikation und frühe Einbindung des CISOs in die strategische und praktische Transformation der Fachabteilungen wird IT-Sicherheit als vollwertiger Geschäftsprozess gelebt und damit in den Köpfen der Unternehmensführung verankert. Nur wenn der CISO über den notwendigen Handelsspielraum verfügt und in Entscheidungen von Bereichsleitern eingebunden wird, kann er die Sicherheitsinteressen des Unternehmens wahrnehmen. In dieser Position unterstützt er sein Unternehmen bei der Schaffung eines ganzheitlichen Risikomanagements und einer angemessenen Umsetzung der digitalen Transformation. Dazu gehört der Schutz von Unternehmensinformationen und IT-Technologien und damit von Menschen (deren Daten in den IT-Systemen abgelegt sind) und Organen vor Bedrohungen.

Fazit

Die Aufgaben IT-Sicherheit und Datenschutz sind von herausragender Bedeutung für die Sicherung der Zukunftsfähigkeit von Unternehmen. Soll diese Aufgabenstellung nachhaltig erfolgreich bewältigt werden, so gehört sie in die Hand eines Verantwortlichen, der auf direktem Wege mit dem Top-Management kommuniziert. Unternehmen, denen es gelingt, IT-Sicherheit in einen Teil ihrer Identität und Firmenkultur zu verwandeln, werden deutlich weniger angreifbar sein als in diesen Bereichen weniger fokussierte Organisationen. Eine wichtige Rolle auf dem Weg dorthin übernimmt ein CISO.

Quellenangaben

[1] Rochus Mummert: Rund die Hälfte der deutschen Unternehmen von Cyber-Kriminalität betroffen, April 2019
https://www.rochusmummert.com/aktuelles/rund-die-haelfte-der-deutschen-unternehmen-von-cyber-kriminalitaet-betroffe/
[2] BSI: Cyber-Sicherheits-Umfrage – Cyber-Risiken & Schutzmaßnahmen in Unternehmen, April 2019
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Cyber-Sicherheits-Umfrage/CyberSicherheitsUmfrage_2018/cs_umfrage_2018_node.html1
[3] Electric Emergency and Disturbance Report - Calendar Year 2019,
https://www.eenews.net/assets/2019/04/30/document_ew_03.pdf
[4] EY: Global Information Security Survey 2018–19, Oktober 2018
https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf
[5] EY: Global Information Security Survey 2018–19, Oktober 2018
https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf
[6] PWC: The Global State of Information Security Survey 2018, November 2018
https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html
[7] CIO.de: The Global State of Information Security 2006: Der Teenager im CISO-Büro, November 2006
https://www.cio.de/a/der-teenager-im-ciso-buero,829264
[8] Rochus Mummert: Rund die Hälfte der deutschen Unternehmen von Cyber-Kriminalität betroffen, April 2019
https://www.rochusmummert.com/aktuelles/rund-die-haelfte-der-deutschen-unternehmen-von-cyber-kriminalitaet-betroffe/
[9] Bundesdruckerei: Digitalisierung und IT-Sicherheit in deutschen Unternehmen, Juni 2017
https://www.bundesdruckerei.de/system/files/dokumente/pdf/Studie-Digitalisierung_und_IT-Sicherheit.pdf
[10] EY: Global Information Security Survey 2018–19, Oktober 2018
https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf
[11] West Monroe Partners: Reshaping Healthcare M&A: How Competition and Technology are Changing the Game, Mai 2018
https://www.westmonroepartners.com/Insights/White-Papers/Healthcare-MA-Survey
[12] BSI: Cyber-Sicherheits-Umfrage – Cyber-Risiken & Schutzmaßnahmen in Unternehmen, April 2019
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Cyber-Sicherheits-Umfrage/CyberSicherheitsUmfrage_2018/cs_umfrage_2018_node.html1

Über Link11

Link11 ist ein im Bereich Business-Continuity führender IT-Sicherheitsanbieter mit Hauptsitz in Deutschland. Über die Cloud-Security-Plattform schützt Link11 die Webseiten und IT-Infrastrukturen mit einer zum Patent angemeldeten Lösung vor Distributed-Denial-of-Service-(DDoS)-Angriffen. Weitere Services wie Web Application Firewall (WAF) oder Content Delivery Network (CDN) runden das Angebot ab. Die internationalen Kunden profitieren so von einem 360° Schutz und maximaler Performance.
Seit der Gründung des Unternehmens im Jahr 2005 wurde Link11 mehrfach für seine innovative Lösung und das starke Wachstum ausgezeichnet.