business factors

LÜNENDONK

Whitepaper

IT-Security in Strategie und Organisation

Wie IT-Security-Verantwortliche den Status quo beurteilen

Eine Publikation von business factors und Lünendonk anlässlich der

StrategieTage ITS IT Security

vom 15/16. Februar 2016 im Schloss Bensberg

Inhaltsverzeichnis

Vorwort

Hartmut Lüerßen,
Partner,
Lünendonk

Dr. Hagen Streb,
Mitglied der Geschäftsleitung,
business factors
Deutschland

Liebe Leserinnen, liebe Leser,

die digitale Transformation sorgt für tiefgreifende Veränderungen von unternehmensübergreifenden Geschäftsprozessen. Neue Partner-Ökosysteme entstehen im Zusammenhang mit neuen Geschäftsmodellen auf der Basis des Internet der Dinge. Mit der Abhängigkeit der Prozesse von der IT steigen auch die Anforderungen an die IT-Security. Parallel dazu steigt nicht nur die Zahl der Cyberangriffe, die die Unternehmen international abwehren müssen. Die Bedrohungsszenarien werden komplexer, die individuellen Angriffe bei lohnenden Zielen deutlich professioneller.

IT-SECURITY-STRATEGIE RÜCKT IN DEN FOKUS

Damit eine IT-Security-Strategie in alle Unternehmensbereiche hinein wirken kann, ist es erforderlich, dass der Stellenwert der IT-Security sowohl in der IT als auch darüber hinaus als hoch und erforderlich angesehen wird. Dafür sind strategische Sichtbarkeit und Verankerung in der Organisation gleichermaßen wichtige Faktoren. Ohne Kraft in der Funktion und der Organisation wird es einem Chief Information Security Officer (CISO) schwer fallen, die IT-Security-Governance auch durchzusetzen, wobei die IT-Security im Aufgabenbereich des CISO eine immer wichtigere Bedeutung erfährt.

Gerade in Zeiten, in denen die Fachbereiche immer mehr IT-relevante Projektbudgets für Projekte steuern und verantworten und die Unternehmensprozesse immer häufiger mit Cloud-Services integriert werden, muss das Verständnis für die Bedeutung der IT-Security über die IT-Abteilung hinaus wirken.

Im Rahmen der StrategieTage IT Security 2016, organisiert von business factors, wurden 76 hochkarätige Entscheider aus Unternehmen mit mehr als 100 Millionen Euro Umsatz zu den Themen IT-Security in Strategie und Organisation befragt. Die Ergebnisse wurden von Lünendonk ausgewertet und analysiert und finden sich in diesem Whitepaper wieder. Damit möchten Lünendonk und business factors Führungskräften einen Überblick verschaffen, wie der Status quo derzeit von den Unternehmen beurteilt wird und welche Handlungsfelder sich daraus ergeben.

Wir wünschen Ihnen eine nützliche Lektüre!
Herzliche Grüße

Hartmut Lüerßen
Partner,
Lünendonk GmbH

Dr. Hagen Streb
Mitglied der
Geschäftsleitung
business factors
Deutschland GmbH

IT-Security als Teil der IT-Strategie

Immer, wenn ein Unternehmen mit den Auswirkungen eines Cybercrime-Angriffs zu kämpfen hat, die Produktion steht oder Datenverluste öffentlichkeitswirksam eingestanden werden müssen, rückt die IT-Security in den Fokus der Aufmerksamkeit – in diesen Fällen leider zu spät.

Damit eine IT-Security-Strategie präventiv wirken kann und das Unternehmen jederzeit über eine Risikobewertung von potentiellen Schwachstellen und tatsächlichen Vorfällen verfügt, ist es zunächst erforderlich, die IT-Security-Strategie zum festen Teil der IT-Strategie zu machen.

Darüber hinaus sollten die Risiken nicht nur aus IT-technischer Perspektive bewertet werden. Weil die wirtschaftlichen und rechtlichen Folgen möglicher Schwachstellen und Versäumnisse der Sorgfaltspflichten existenzbedrohend für das Unternehmen und strafrechtlich relevant für die Geschäftsführer und Vorstände sein können, gehören auch diese Analysen zu einer umfassenden IT-Security-Strategie.

Dass diese Bewertungen keine Einmal-Aufgabe sind, sondern regelmäßig bei Veränderungen in den Prozess- und Organisationsstrukturen erneuert werden müssen, liegt auf der Hand.

Von den befragten 76 Unternehmen haben 87 Prozent die IT-Security-Strategie als festen Teil der IT-Strategie implementiert. Damit hat das Thema auf der IT-strategischen Ebene in diesen Unternehmen zumindest einmal die erforderliche Sichtbarkeit und Bedeutung. Über die Qualität der Umsetzung und organisatorischen Durchsetzungsfähigkeit der Regeln kann an dieser Stelle keine Aussage getroffen werden.

Dass immerhin 13 Prozent der Unternehmen die IT-Security-Strategie unabhängig von der IT-Strategie betrachten, deutet darauf hin, dass hier ein durchgängiger Ansatz über die verschiedenen Unternehmensbereiche und Prozesslandschaften nur schwer umgesetzt werden kann. Diese Unternehmen gehören bezogen auf die Umsatzgröße zum gehobenen Mittelstand. Bei den Unternehmen mit mehr als 3 Milliarden Euro Umsatz gehört die IT-Security-Strategie immer als fester Bestandteil zur IT-Strategie.

Fast alle der Unternehmen, die die IT-Security-Strategie als Teil der IT-Strategie entwickeln, führen auch rechtliche und wirtschaftliche Risikobewertungen im Rahmen der IT-Security-Strategie durch. Zwei Unternehmen, die die IT-Security-Strategie als Teil der IT-Strategie entwickeln, haben bei dieser Frage nicht geantwortet. Weitere zwei Unternehmen, die die IT-Security-Strategie als Teil der IT-Strategie entwickeln, führen keine rechtlichen und wirtschaftlichen Risikobewertungen durch.

Es zeigt sich, dass im gehobenen Mittelstand teilweise noch Nachholbedarf in Bezug auf den Stellenwert der IT-Security-Strategie besteht.

DIE MEISTEN UNTERNEHMEN HABEN DIE IT-SECURITY-STRATEGIE ALS TEIL DER IT-STRATEGIE ETABLIERT

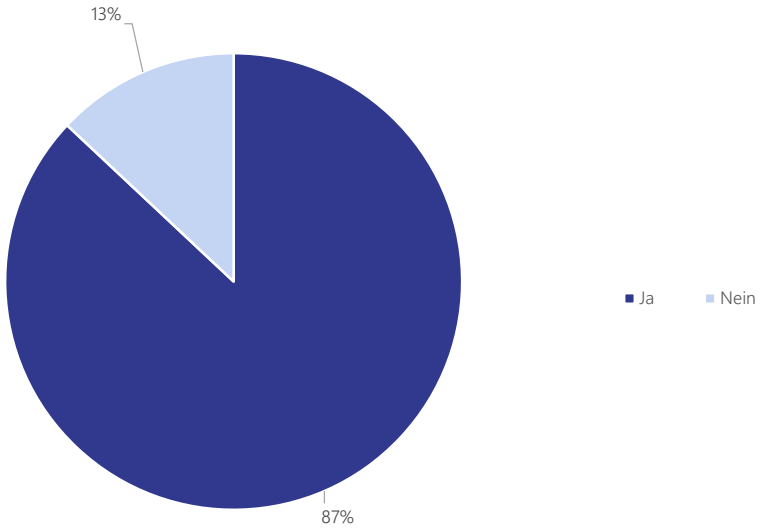

Abbildung 1: Frage: Ist die IT-Security-Strategie Teil der IT-Strategie Ihres Unternehmens? n= 76

RECHTLICHE UND WIRTSCHAFTLICHE RISIKOBEWERTUNG IM RAHMEN DER IT-SECURITY-STRATEGIE SIND WEIT VERBREITET

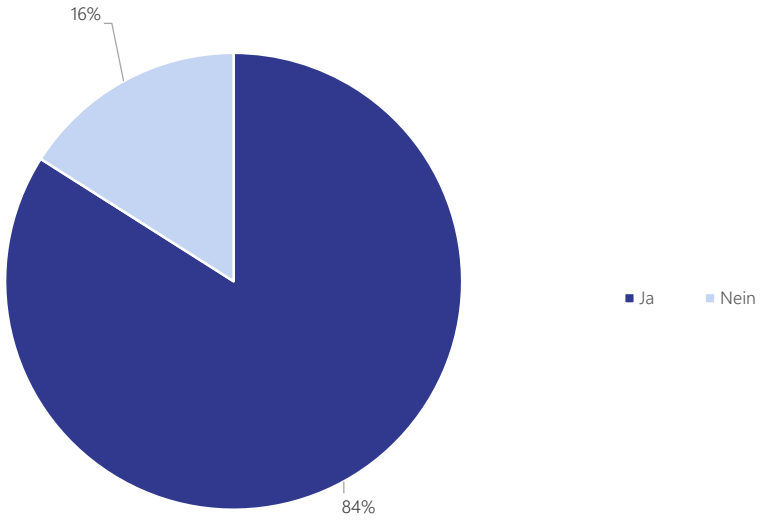

Abbildung 2: Frage: Wurden im Rahmen der IT-Security-Strategie auch rechtliche und wirtschaftliche Risiken für das Unternehmen bei Verstößen und Datenverlusten bewertet? n= 74

Die Rolle der IT-Security in der Organisation

Zwei wesentliche Gradmesser der Bedeutung der IT-Security im Unternehmen sind die Funktion des Chief Information Security Officers (CISO) sowie seine Position und Berichtswege in der Organisation. Dabei sollte in der Praxis zwischen formaler und tatsächlicher Bedeutung unterschieden werden: Entspricht die tatsächliche Bedeutung und Handlungsfähigkeit der formalen Bedeutung in der Organisation?

Um diese Übereinstimmung zu überprüfen, eignet sich ein einfacher Praxistest: über die Beteiligung an den „Was“- und den „Wie“-Fragen bei strategischen Projekten. Wird die IT-Security bei wichtigen Projekten bereits bei den strategischen Projektanforderungen mit berücksichtigt (also bei den „Was“-Fragen“) oder erst im Laufe des Projektes, beispielsweise im Rahmen der Testanforderungen („Wie“-Fragen)?

Die Was-Fragen sind die Fragen und Anforderungen, denen das Projektleitungsgremium von Beginn an große Bedeutung beimisst. Die Wie-Fragen betreffen vor allem Fragen der Umsetzung, die für den Projekterfolg nicht weniger kritisch sein können, jedoch in der Tiefe nur bei Bedarf vom Projektleitungsgremium verfolgt werden.

Aus der formalen Perspektive heraus gibt es bei den befragten Unternehmen in 88 Prozent der Fälle einen CISO. Bei 12 Prozent der Unternehmen ist die Rolle eines CISO nicht etabliert. Dabei berichtet der CISO am häufigsten an den CIO (49 %). Immerhin bei 39 Prozent der Unternehmen berichtet der CISO sogar direkt an den Vorstand, was seiner Rolle im Unternehmen zusätzliches Gewicht verleiht und die funktionale Trennung der Informationssicherheit von der IT etabliert.

CISO BERICHTET AM HÄUFIGSTEN AN DEN CIO

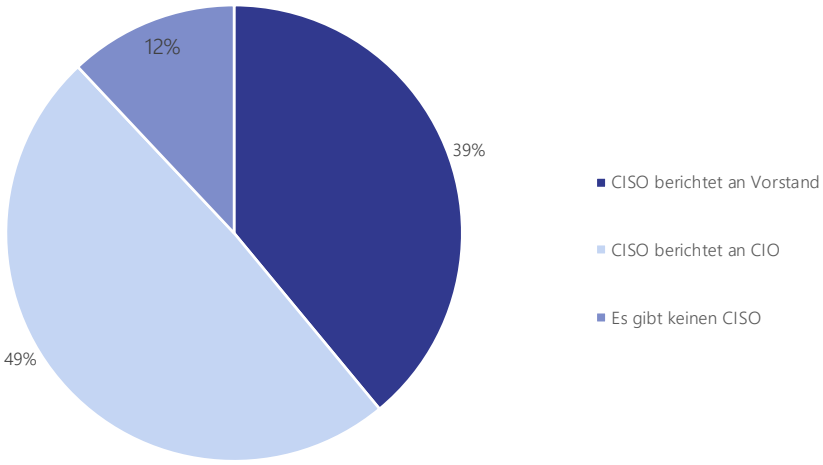

Abbildung 3: Frage: An wen berichtet der CISO in Ihrem Unternehmen? n=69

Da in vielen Unternehmen die CIO-Funktion nicht auf Vorstandsebene etabliert ist, besteht hier aus der Marktperspektive noch deutlicher Nachholbedarf: Die IT hat eine unternehmenskritische Bedeutung, trotzdem ist der Berichtsweg des CISO an den Vorstand oft indirekt.

Es gibt Vor- und Nachteile, wenn der CISO an den CIO berichtet. Für eine unabhängige Funktion mit teilweise unangenehmen Governance-Forderungen an die IT kann eine hierarchische Eingliederung in die IT-Struktur zu Interessenkonflikten führen. Der Vorteil eines CISO innerhalb der IT liegt hingegen in der direkten Einbindung in die Projekt- und IT-Services-Prozesse. Auch eine Einbindung der CISO-Funktion in die IT mit direktem Berichtsweg an den Vorstand kommt vor und hat Vorteile, wenn der CIO beispielsweise nicht Teil des Vorstandes ist.

Entscheidend im Zusammenhang mit der Digitalen Transformation ist in jedem Fall ein hohes und damit zu steigerndes Bewusstsein für die Bedeutung der IT-Security. Diese muss aktiv gefördert werden. Internes Marketing ist daher eine wichtige Aufgabe für die CISOs. Das gilt vor allem dann, wenn die Vorstands- und Geschäftsführungsebene die Digitale Transformation mit Verzögerung angeht. Großer Zeitdruck ist eine der größten Gefahren für die Einhaltung von IT-Security-Anforderungen und Qualitätssicherung.

Für die Unternehmen mit mangelndem IT-Security-Bewusstsein stellt sich die Frage, ob erst ein großer Schaden eintreten muss oder die Überzeugungskraft des CISO ausreicht, um die IT-Security umfassender zu berücksichtigen?

Methodik und Stichprobenverteilung

Die Befragung wurde im Vorfeld der von business factors organisierten StrategieTage IT Security 2016 durchgeführt. Hierzu wurden die Konferenzteilnehmer angeschrieben und gebeten, Fragen zu ihren Themenschwerpunkten sowie ihre Einschätzung der Bedeutung der IT-Security in Strategie und Organisation zu äußern. 76 Teilnehmer haben sich an der Befragung beteiligt.

Die Antworten wurden von Lünendonk ausgewertet und analysiert. Die 76 Teilnehmer repräsentieren überwiegend große mittelständische Unternehmen mit einem Umsatz zwischen 100 Millionen Euro und bis zu 3 Milliarden Euro weltweit im Jahr 2015 (67 Prozent). Weitere 33 Prozent der Befragten repräsentieren große Unternehmen mit mehr als 3 Milliarden Euro weltweitem Umsatz im Jahr 2015. Viele dieser Unternehmen haben Konzernstrukturen.

Die Ergebnisse des Whitepapers geben daher einen guten Einblick in die Planung und den Status quo bei Unternehmen des gehobenen Mittelstands und Konzernen.

DIE UNTERNEHMEN REPRÄSENTIEREN DEN GEHOBENEN MITTELSTAND UND GROßE UNTERNEHMEN

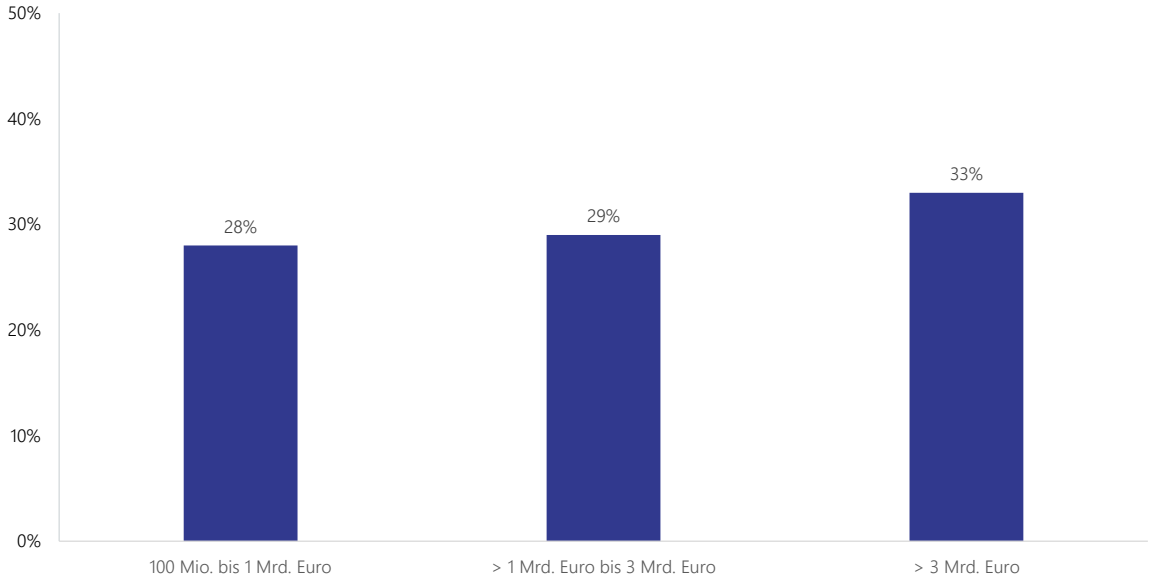

Abbildung 4: Die Teilnehmerunternehmen der Befragung verteilen sich gleichmäßig auf die Umsatzgrößenklassen. N=76

Bezogen auf die befragten Funktionen zeigt sich bei den Befragungsteilnehmern ein hohes Entscheiderniveau. So sind mehr als 57 Prozent der Befragten CISO oder CIO in ihren Unternehmen.

Weitere 26 Prozent gehören dem gehobenen IT-Management in unterschiedlichen Bereichen von IT-Infrastruktur bis Anwendungsentwicklung an. 17 Prozent der Befragten sind im Bereich IT-Security-Management überwiegend operativ für die IT-Security verantwortlich.

Damit ist die Zielgruppe in der Lage, sehr fundierte Auskunft über die Bedeutung der IT-Security in Strategie und Organisation in den Unternehmen zu geben.

DIE BEFRAGUNGSTEILNEHMER REPRÄSENTIEREN EINE HOHE ENTSCHEIDEREBENE IN DEN UNTERNEHMEN

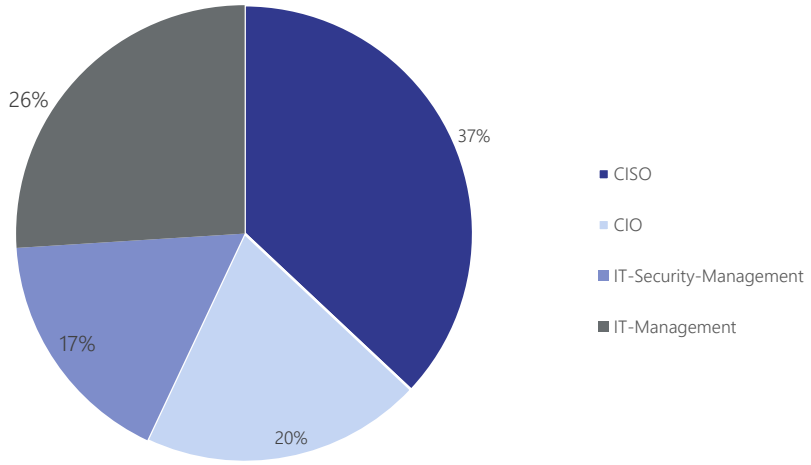

Abbildung 5: Mehr als 57 Prozent der Befragten sind CISO oder CIO. N=76

UNTERNEHMENSPROFIL

business factors Deutschland

business factors schafft exklusive Kommunikationsräume für hochrangige Führungskräfte deutscher und internationaler Unternehmen.

Unser Leistungsspektrum umfasst die Konzeption, Organisation und Umsetzung von Wirtschaftskongressen basierend auf einem umfangreichen Führungskräftenetzwerk und passgenauen IT-gestützten Matchingprozessen für die Abgleichung von Interessen, Herausforderungen und Lösungen.

Als unabhängiger Veranstalter zeichnen wir mit den StrategieTagen auf Schloss Bensberg und in Zürich verantwortlich für maßgebende Kongresse in den Bereichen IT, HR, Vertrieb, Marketing, Kundenmanagement, Energie, Industrie und Finance. Diese bieten Führungskräften exzellente Möglichkeiten, sich umfassend zu informieren, auszutauschen und zu den entscheidenden Themen zu vernetzen.

Unsere Büros in Berlin, Bergisch Gladbach, Warschau und den Vereinigten Arabischen Emiraten gewährleisten die internationale Einbettung unserer D.A.CH. Kongresse ebenso wie die Etablierung neuer Veranstaltungsformate im EMEA-Raum.

KONTAKT

business factors Deutschland GmbH
Dr. Hagen Streb
Mitglied der Geschäftsleitung
Tauentzienstraße 15, 10789 Berlin
Telefon: +49 30 2005136-13
Telefax: +49 30 2005136-29
E-Mail: hagen.streb@businessfactors.de
Internet: www.businessfactors.de

UNTERNEHMENSPROFIL

LÜNENDONK

Lünendonk

Die Lünendonk GmbH, Gesellschaft für Information und Kommunikation (Kaufbeuren), untersucht und berät europaweit Unternehmen aus der Informationstechnik-, Beratungs- und Dienstleistungsbranche. Mit dem Konzept Kompetenz[3] bietet Lünendonk unabhängige Marktforschung, Marktanalyse und Marktberatung aus einer Hand. Der Geschäftsbereich Marktanalysen betreut seit 1983 die als Marktbarometer geltenden Lünendonk®-Listen und -Studien sowie das gesamte Marktbeobachtungsprogramm.

Die Lünendonk®-Studien gehören als Teil des Leistungsportfolios der Lünendonk GmbH zum „Strategic Data Research“ (SDR). In Verbindung mit den Leistungen in den Portfolioelementen „Strategic Roadmap Requirements“ (SRR) und „Strategic Transformation Services“ (STS) ist Lünendonk in der Lage, ihre Beratungskunden von der Entwicklung der strategischen Fragen über die Gewinnung und Analyse der erforderlichen Informationen bis hin zur Aktivierung der Ergebnisse im operativen Tagesgeschäft zu unterstützen.

KONTAKT
Lünendonk GmbH
Gesellschaft für Information und Kommunikation
Hartmut Lüerßen
Partner
Maximilianstraße 40, 87719 Mindelheim
Telefon: +49 8261 73140-0
Telefax: +49 8261 73140-66
E-Mail: lueerssen@luenendonk.de
Internet: www.luenendonk.de

LÜNENDONK

ÜBER LÜNENDONK

Seit 1983 ist die Lünendonk GmbH spezialisiert auf systematische Marktforschung, Branchen- und Unternehmensanalysen sowie Marktberatung für Informationstechnik-, Beratungs- und weitere hochqualifizierte Dienstleistungsunternehmen. Der Geschäftsbereich Marktforschung betreut die seit Jahrzehnten als Marktbarometer geltenden Lünendonk®-Listen und -Studien sowie das gesamte Marktbeobachtungsprogramm. Die Lünendonk®-Studien gehören als Teil des Leistungsportfolios der Lünendonk GmbH zum „Strategic Data Research" (SDR). In Verbindung mit den Leistungen in den Portfolio-Elementen „Strategic Roadmap Requirements" (SRR) und „Strategic Transformation Services" (STS) ist die Lünendonk GmbH in der Lage, ihre Kunden von der Entwicklung strategischer Fragen über die Gewinnung und Analyse der erforderlichen Informationen bis hin zur Aktivierung der Ergebnisse im operativen Tagesgeschäft zu unterstützen.

- Managementberatung
- Informations- und Kommunikations-Technik
- Wirtschaftsprüfung / Steuerberatung
- Technologie-Beratung / Engeneering Services
- Zeitarbeit / Personaldienstleistungen
- Facility Management / Industrieservice

LÜNENDONK GMBH
Maximilianstraße 40
D-87719 Mindelheim
Telefon: +49 8261 73140-0
Telefax: +49 8261 73140-66
E-Mail: info@luenendonk.de
Internet: http://www.luenendonk.de

Erfahren Sie mehr unter

www.luenendonk.de

MARKTFORSCHUNG UND MARKTBERATUNG AUS EINER HAND