Deloitte.

Rüstzeug für das Topmanagement
Aufbau eines effektiven Cyber-Security-Programms

Rüstzeug für das Topmanagement
Aufbau eines effektiven Cyber-Security-Programms

Inhaltsverzeichnis

Einleitung

In den vergangenen Jahren haben Unternehmen die Chancen der sich immer weiter verbessernden IT-Systeme genutzt und mit der zunehmenden Digitalisierung der Unternehmensprozesse zusätzliche Angebote für die Kunden geschaffen und unternehmensintern durch die Integration von IT in alle Geschäftsprozesse Effizienzgewinne erzielt. Dieser Trend hat bei den Unternehmen spiegelbildlich zu einer verstärkten Abhängigkeit von den immer komplexeren IT-Systemen geführt, die auch zu neuen Risiken führt und neue Verwundbarkeiten schafft. Cyber-Security ist damit eine der komplexesten Herausforderungen, denen sich Unternehmen aktuell stellen müssen. Vorbei sind aber die Zeiten, in denen sich IT Security auf eine anständige Anti-Virensoftware und eine aktuelle Firewall beschränkte. Das Thema Cyber-Security ist allgegenwärtig und hat sich zu einer wichtigen Aufgabe der Unternehmensführung entwickelt. Damit wird Cyber-Security auch ein Thema für Aufsichtsräte, die im Rahmen ihrer Aufgaben zur Unternehmensüberwachung sicherstellen müssen, dass dieses neue Thema und die neuen Gefahren angemessen von der Unternehmensführung beachtet und bewältigt werden. Damit muss sich nicht nur die Unternehmensführung, sondern auch der Aufsichtsrat intensiv mit diesem Thema auseinandersetzen.

In den vergangenen Jahren haben Cyber-Angriffe, bei denen geschützte Informationen entwendet oder IT-Infrastrukturen gestört wurden, stark zugenommen. Die rasante Entwicklung neuer Technologien und Kommunikationsformen, wie Cloud-Computing und Social Media, haben die Angriffsfläche von Unternehmen zusätzlich verbreitert und verändern somit die Risikolandschaft der Unternehmen dramatisch.

Laut der polizeilichen Kriminalstatistik 2012 ist die Zahl an Cyber-Straftaten in Deutschland gegenüber 2011 um 7,5 Prozent auf rund 64.000 gestiegen. Im Vergleich zum Zeitraum seit 2007 entspricht der Anstieg sogar 87 Prozent.

Derartige Straftaten, insbesondere wenn geistiges Eigentum entwendet wird, können die Marktposition und das Image eines Unternehmens negativ beeinflussen. Und Cyber-Attacken gehen auch häufig mit erheblichen finanziellen Auswirkungen einher, da die Angriffe das Vertrauen der Kunden und Geschäftspartner in den erwarteten Umgang mit Informationen nachhaltig schädigen.[1]

Der Deutsche Corporate Governance Kodex weist dem Vorstand und damit der Unternehmensführung die klare Verantwortung für das Risikomanagement des Unternehmens zu (DCGK 4.1.4), dem auch die Informationssicherheit zugerechnet wird. Die Aufgabe des Aufsichtsrates ist es, den Vorstand zu überwachen, so dass auch das System des Risikomanagements und damit die IT-Sicherheit auf die Agenda des Aufsichtsrates gehören. Internationale Studien[2] belegen allerdings, dass es innerhalb des Organs der Unternehmensführung und -überwachung Unterschiede im Verständnis der Verbindung von IT-Risiken mit Unternehmensrisiken gibt. Der Unternehmensführung sowie den überwachenden Organmitgliedern fehlt darüber hinaus vielfach die Übersicht über Aktivitäten ihrer Unternehmen zu Themen wie Cyber-Security, Sicherheitsprogrammen, Top-Level Policies, Verantwortlichkeiten für Daten- und Informationsschutz sowie Budgetkontrolle. Laut dieser Studie erhalten die Unternehmensorgane bisher außerdem zu selten regelmäßige Berichte über Verstöße und Risiken in der Informationssicherheit.

Die Ergebnisse dieser Studie aus den USA können nach unserer Einschätzung ohne Einschränkung auf die Unternehmensführung und die Aufsichtsräte deutscher Unternehmen übertragen werden, wenngleich nach unseren Beratererfahrungen Deutschland hier noch deutlich Aufholbedarf hat.

Und oft liegt es nicht am mangelnden Informationsfluss, sondern an nicht erkannten Attacken auf IT-Systeme und IT-Netzwerke. Denn vielfach fehlt den Unternehmen und ihren Mitarbeitern schlicht das erforderliche Know-how, um Cyber-Straftaten selbst erkennen zu können. Eine Studie des Verizon RISK Teams aus dem Jahr 2011 zeigt, dass ein Großteil der Unternehmen, die gehackt wurden (86%), nicht selbst den Angriff auf das eigene Unternehmensnetzwerk registriert hat, sondern externe Dritte (z.B. Vollzugsbehörden) oder externe „Fraud Detection"-Programme den Angriff aufdeckten.[3]

[1] "Second annual cost of cyber crime study," 2011, p.1.

[2] Vgl. z.B. "Governance of Enterprise Security: CyLab 2012 Report", Carnegie Mellon University; Available online at http://globalcyberrisk.com/wp-content/uploads/2012/08/CMU-GOVERNANCE-RPT-2012-FINAL1.pdf.

[3] 2011 data breach investigations report: A study conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit," Verizon, 2011. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf.

Die amerikanische Börsenaufsicht (Securities and Exchange Commission (SEC)) legt zunehmend Wert darauf, dass Unternehmen Angaben im Konzernabschluss und in der Risikoberichterstattung über den Umgang mit dem Risiko Cyber-Security, die Auswirkungen potenzieller Risiken und insbesondere Cyber Incidents machen.[4]

Es ist die Aufgabe der Unternehmensführung - bei einer AG der Vorstand und bei einer GmbH die Geschäftsführung – sicherzustellen, dass das Unternehmen auf potentielle Cyber-Angriffe vorbereitet ist, tatsächlichen Cyber-Angriffen zu begegnen, auf diese zu reagieren sowie den damit verbundenen regulatorischen Anforderungen und geschäftlichen Entwicklungen gerecht zu werden. Der Aufsichtsrat als Überwachungsinstanz hat sich zu vergewissern, dass die Unternehmensführung ihrer Verantwortung entsprechend nachkommt.

„Ein wirksamer Schutz vor Cyber-Angriffen ist nur möglich, wenn Gefährdungen im Cyber-Raum sowie die eigene tatsächliche Gefährdungslage zumindest im Überblick bekannt sind“

Register aktueller Cyber-Gefährdungen und -Angriffsformen, BSI (2012)

Diese Publikation stellt dar, welchen Herausforderungen sich Unternehmen und die Unternehmensführung in der Informationssicherheit gegenübergestellt sehen und wie sich Organisationen auf aktuelle und künftige Bedrohungen einstellen müssen. Insbesondere zeigen die Autoren die Verantwortlichkeiten für unterschiedliche Aufgabenbereiche der Cyber-Security innerhalb des Unternehmens auf und beleuchten hierbei vor allem die Funktion der Unternehmensführung und des Aufsichtsrats.

[4] Vgl. http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

Typische Cyber-Attacken – wer sind die Täter?

Die zahlreichen Angriffsarten sind von unterschiedlichen Zielen der Angreifer geleitet. Die Täter sind oft Einzelpersonen oder kleine Gruppen, z.B. Insider, Lieferanten und Aktivisten, aber auch professionelle kriminelle Netzwerke oder staatlich gelenkte Organisationen. Die Motivation hinter den Angriffen reicht von Finanzbetrug, Datendiebstahl und -missbrauch, Aktivismus, Sabotage bis zur gezielten Spionage.

Die Täter bedienen sich bei Angriffen meist verschiedener Techniken, die häufig kombiniert werden. Hierzu zählen z.B. das Einschleusen von Schadsoftware (Viren, Würmer, Trojaner, Spyware), das „Phishing" von Passwörtern oder Denial-of-Service-Attacken.

Jede Angriffsart stellt eine besondere Gefahr dar, gegen die gezielt Vorkehrungen getroffen werden müssen. Nicht alle Vorkehrungen sind hierbei technischer Natur: Durch „Social Engineering" oder „Phishing" lassen sich Mitarbeiter oder Kunden teilweise Informationen entlocken, die sie unter normalen Umständen nicht preisgeben würden. Daher spielt das Bewusstsein für derartige Gefahren sowie die Kenntnis bestehender Unternehmensrichtlinien eine zentrale Rolle. Das Bewusstsein sollte durch regelmäßige, unternehmensweite Schulungen der Mitarbeiter und gezielte Information der Kunden gestärkt werden.

63.959 **Fälle von Cyberkriminalität 2012**

+ 7,5% gegenüber 2011
+ 87% seit 2007

Quelle: Polizeiliche Kriminalstatistik 2012

Verantwortlichkeiten für Cyber-Security innerhalb des Unternehmens

Cyber-Security wird im Idealfall im Unternehmen von mehreren Ebenen und Ansprechpartnern adressiert. Dies macht einerseits die Suche nach dem „Verantwortlichen" nicht immer leicht, zeigt aber auch gleichzeitig auf, dass es sich um ein Querschnittsthema handelt, für das das Unternehmen als Gesamtes einen Plan haben sollte. Welche Rolle spielen die verschiedenen Akteure?

Unternehmensführung

Die Mitglieder der Unternehmensführung – bei einer AG der Vorstand und bei einer GmbH die Geschäftsführung – sollten über den Stand des Cyber-Security-Programms im Bilde sein und im Falle eines Cyber-Angriffs wissen, welche Schritte durchzuführen sind und welche Mitarbeiter in dieser Situation Schlüsselpositionen besetzen. In den meisten Unternehmen ist eine Person aus der Unternehmensleitung als konkreter Ansprechpartner für Informationssicherheit festgelegt – häufig der Chief Information Officer (CIO). Alternativ wird ein Chief Security Officer (CSO) oder auch der Datenschutzbeauftragte, der zusätzlich das Thema physische Sicherheit verantwortet, mit der Aufgabe betraut. Immer häufiger wird der Chief Information Security Officer (CISO) als Dreh- und Angelpunkt mit dem Fokusthema Cyber-Security eingesetzt. In der Regel berichten diese Funktionen direkt an den Vorstand bzw. die Geschäftsführung. Sie sind in jedem Fall aber die idealen Ansprechpartner für Vorstand und Aufsichtsrat zu Risiken und Cyber-Angriffen.

Interne Revision

Die Unternehmensführung ist dafür verantwortlich, dass im Unternehmen eine angemessene und wirksame Interne Revision besteht. Dabei wird die Unternehmensleitung in der Regel sicherstellen, dass die Interne Revision regelmäßig die umgesetzten Kontrollen für Cyber-Sicherheit auf ihre Aktualität, Relevanz und Effektivität überprüft.

Der Aufsichtsrat ist auch für die Überwachung der Wirksamkeit des Internen Revisionssystems zuständig (§ 107 Abs. 3 S. 2 AktG). Ein Aufsichtsrat wird sich daher auch mit den Fragen beschäftigen, ob, inwieweit und mit welchen Mitteln sich die Interne Revision mit dem Thema Cyber-Security beschäftigt.

Externer Prüfer

Externe Prüfer – als fachliche Unterstützung der Internen Revision oder im Auftrag des CISO – können in vielen Fällen eine wertvolle Unterstützung zum Thema Cyber-Security sein. Dies insbesondere in den Fällen, in denen ein Unternehmen nicht oder noch nicht über das notwendige Know how und die notwendigen Kapazitäten auf dem Gebiet der Cyber-Security verfügt. Manche externen Dienstleister und Berater haben sich darauf spezialisiert, Sicherheitsmaßnahmen zu bewerten und die kontinuierliche Verbesserung zu unterstützen. Externe Prüfer greifen auf einen umfangreichen Erfahrungsschatz aus verschiedensten Unternehmen und Wirtschaftszweigen zurück und können so verschiedene Perspektiven einbringen.

Externe Spezialisten

Hilfreich ist es auch, sich durch externe Spezialisten bei der Überprüfung und Umsetzung von Sicherheitsmaßnahmen beraten zu lassen. Sie führen Security-Assessments durch, prüfen und beurteilen dabei die vorhandenen Sicherheitsprogramme des Unternehmens und helfen bei der Planung und Umsetzung adäquater Maßnahmen. Sogenannte „Third-Party Security Assessments" ermöglichen darüber hinaus ein Benchmarking zu anderen Gesellschaften gleicher Größe und/oder Branche.

Aufsichtsrat

Ein erfolgreiches Cyber-Security-Programm erfordert regelmäßiges, proaktives Engagement durch den Aufsichtsrat. Er spielt eine wichtige Rolle bei der Überwachung der Management-Aktivitäten auf dem Gebiet der Cyber-Security und der Beurteilung ihrer Wirksamkeit, da er den nötigen Überblick über das gesamte Unternehmen hat. Darüber hinaus sollte der Aufsichtsrat Wert darauf legen, dass die Unternehmensführung sicherstellt, dass Mitarbeiter in verantwortungsvoller Position über das erforderliche Know-how in den Bereichen IT-Security, Security-Governance und Cyber-Risk verfügen.

In den USA hat sich der Trend manifestiert, dass das Board of Directors ein dediziertes Risikokomitee mit dem Fokus auf Sicherheit und Informationsschutz etabliert.[5] In Deutschland ist es allerdings häufig Praxis, das Thema Cyber-Security dem Prüfungsausschuss zu übertragen.

[5] Governance of Enterprise Security: CyLab 2012 Report (Carnegie Mellon University CyLab).

Fragen zum Thema Cyber-Security

Wie gut ist ein Unternehmen bereits geschützt?
Die Checkliste berücksichtigt die wichtigsten Inhalte einer Cyber-Strategie.

Hat Ihr Unternehmen eine Informations- und Cyber-Strategie zum Schutz der Informationswerte und kennen Sie sie?	❍
Kennen Sie die kritischen Informationswerte und die damit verbundenen Risiken? Wie werden diese Risiken identifiziert, bewertet und behandelt?	❍
Verlassen digitale Informationen das Unternehmen und werden diese Datenflüsse überwacht?	❍
Ist bekannt, wer sich von wo in das Unternehmensnetzwerk einloggt und ob die Informationen, die hierbei abgerufen werden, vom jeweiligen Benutzer angesehen werden dürfen?	❍
Sind die Incident-Response- und Kommunikationspläne des Unternehmens stabil?	❍
Werden Bestimmungen und regulatorische Anforderungen eingehalten – besonders im Zusammenhang mit Informationssicherheit und Datenschutz?	❍
Haben Sie für den Betrieb und den Datenaustausch mit Cloud- und Zuliefernetzwerken Kontrollen eingeführt?	❍
Sind Software und Informationen auf unternehmenseigenen Geräten wie Laptops und Smartphones gesichert?	❍
Wird kontrolliert, welche Software auf welchen Geräten installiert ist?	❍
Sind alle Mitarbeiter für ihre Aufgabe ausgebildet, um Cyber-Risiken abschätzen und prognostizieren zu können?	❍
Haben Sie ein regeläßiges und unternehmensweites Training für alle Mitarbeiter etabliert oder eine Kampagne zum Thema Informations- und Cyber-Security etabliert? Schaffen Sie dadurch das erforderliche (Risiko-)Bewusstsein bei den Mitarbeitern und beim Management?	❍

Erstellung eines effektiven Cyber-Security-Programms

Ein effektives Cyber-Security Programm umfasst den gesamten Zyklus der Informationsverarbeitung und geht über die klassischen präventiven IT-Security-Schutzmaßnahmen hinaus. Der Deloitte-Ansatz für Cyber-Security umfasst drei Phasen:

- Prepare – die Vorbereitung
- Aware – der laufende Betrieb
- Respond – die richtige Reaktion im Fall der Fälle

Prepare

Die umfassende Vorbereitung auf das Offensichtliche ist Pflicht, denn sonst ist man schon verloren und etwaige IT-Security-Maßnahmen werden Makulatur. Bei der Vorbereitung werden einmal alle Sicherheitstechnologien auf ihre technische Standhaftigkeit sowie die Software-Stände und deren Konfiguration auf ihre Aktualität überprüft. Daraus muss die IT einen laufenden Prozess gestalten, durch den die Systeme fortwährend gegen neu aufkommende Software-Schwächen abgesichert werden.

Der aufwändigere Bereich umfasst die Abläufe um das Sicherheitsmanagement. Es ist naheliegend, dass man sich auf den Ernstfall vorbereitet und die Meldeketten im Unternehmen, aber auch zu den Behörden durchplant und am besten auch in Angriffssimulationen „durchspielt". In unseren Projekten erleben wir hierbei oft sehr heilsame Aha-Effekte, wenn den Teilnehmern die Abhängigkeiten zwischen dem Vertrieb, der IT, der Personalabteilung oder auch den Geschäftspartnern aufgezeigt werden.

Aware

Als weitere Maßnahmen sind die laufende Überwachung kritischer System- und Anwendungsaktivitäten und die Auswertung von Verkehrsverhaltensmustern im Unternehmensnetzwerk unerlässlich. Hierbei geht es nicht darum, die Aktivitäten von Mitarbeitern auszuspionieren, sondern, ob unübliche Systemzugriffe oder Daten(ab)flüsse erfolgen oder einfach Anomalien im IT-Betrieb auftreten. So ist es doch eine Erklärung wert, wenn von einem Server im internen Netzwerk plötzlich sehr große Mengen an Excel- und PowerPoint-Dateien an eine unbekannte Adresse im Internet kopiert werden. Das Beispiel klingt sehr banal, aber ohne geeignete Monitoring-Methoden wird ein Unternehmen den Datenabfluss nie bemerken.

Respond

Wie im richtigen Leben wird man nach einem Einbruch versuchen, die Spuren der Einbrecher nachzuvollziehen. Ziel dabei ist es, einerseits die möglichen Täter zu identifizieren. Noch viel wichtiger ist jedoch die Zielsetzung, die Spuren auszuwerten, um wirklich alle Einfallstore zu identifizieren. Und am Ende müssen alle Systeme so bereinigt werden, dass die Eindringlinge nicht wieder über Hintertüren zurückkommen können.

In allen drei Phasen finden sich wichtige Punkte für einen Managementplan wieder: Im Falle eines Angriffs sind die ersten 48 Stunden entscheidend. Voraussetzung ist, dass das Unternehmen auf mögliche Angriffe vorbereitet wird.

Und zu guter Letzt erfordert ein Cyber-Security-Plan eine entsprechende Kultur, die ein Bewusstsein für die Bedeutung von Cyber-Security beinhaltet, der von der Führungsebene vorgelebt und von allen Mitarbeitern des Unternehmens getragen wird.

Tipps für die Umsetzung des Cyber-Security-Programms

1 Fokussieren Sie die Maßnahmen im ersten Schritt auf die wirklich kritischen Unternehmensinformationen. Fragen Sie sich, welche Auswirkungen ein Angriff auf Ihr Unternehmen haben könnte und was in diesem Fall unternommen werden sollte.

2 Bewerten Sie den Cyber-Incident-Response-Plan und spielen Sie ihn durch. Verstehen Sie, wo Verwundbarkeiten identifiziert und welche Maßnahmen ergriffen wurden, um sie zu entschärfen. Achten Sie auf Schwächen hinsichtlich der Konsistenz der Kontrollen.

3 Manchmal wird das Budget für Sicherheit zum Wohle von anderen IT- oder Unternehmensprojekten vernachlässigt; deshalb sollte jährlich überprüft werden, ob das Cyber-Sicherheitsbudget zielführend eingesetzt und auch tatsächlich genutzt wurde.

4 Lassen Sie sich vom Senior Management zu den Themen der Abwehrbereitschaft, der Erkenntnisse beim Monitoring und der Risiken für Sicherheit und Datenschutz in Form von Key-Risk-Indikatoren unterrichten.

5 Arbeiten Sie mit internen und externen Spezialisten zusammen, um mit den aktuellen Entwicklungen im Bereich Technologie und Cyber-Security vertraut zu sein. Der Aufsichtsrat sollte über neu aufkommende Gefahren unterrichtet werden.

6 Stellen Sie sicher, dass die Datenschutz- und Sicherheitsbestimmungen externer Anbieter – wie Cloud und Hosting Provider – die Bestimmungen Ihres Unternehmens befolgen. Achten Sie besonders auf die Kommunikation, die im Falle eines Sicherheitsvorfalls geplant ist.

7 Bleiben Sie auf dem neuesten Stand hinsichtlich Cyber-Bedrohungen und möglicher Auswirkungen auf Ihr Unternehmen. Verfolgen Sie regelmäßig die Verabschiedung von Gesetzen/Regularien in Bezug auf Cyber-Security.

8 Untersuchen Sie regelmäßig den Nutzen und die Notwendigkeit einer Cyber-Versicherung für die identifizierten Risiken.

Fazit

Noch vor ein paar Jahren waren Unternehmensführung und Aufsichtsrat selten mit dem Thema Cyber-Security befasst. Dies war in der Vergangenheit ein Thema von Fachspezialisten. Sich rasant weiterentwickelnde Technologien, geänderte Arbeitsbedingungen mit Zugang zu Unternehmensinformationen von überall auf der Welt in Verbindung mit verbesserten Angriffstechniken von Kriminellen machen es erforderlich, dass auch die Unternehmensführung und der Aufsichtsrat sich dieser Thematik annehmen und pro-aktiv handeln. Cyber-Security ist eines der Top-Unternehmensrisiken[6] überhaupt und kann nicht länger ausschließlich als IT-Risiko angesehen werden.

Unternehmensinterne und -externe Cyber-Security-Spezialisten entwickeln ausgereifte Ansätze zur Gefahrenabwehr, dem Erkennen von und der Reaktion auf Cyber-Angriffe. Leider können sie aber nicht alle Herausforderungen adressieren, die durch Cyber-Bedrohungen entstehen. Daher ist es wichtig, Kontrollen gezielt an den sich ändernden Bedrohungen auszurichten, laufend zu überwachen und regelmäßig zu überprüfen um im Falle eines Falles vorbereitet zu sein.

„Es gibt zwei Arten von Unternehmen – die, die bereits gehackt wurden, und die Unternehmen, die noch gehackt werden."

Robert Mueller, Direktor des FBI, zur Zukunft von Cyber-Security

[6] Global Risks Report 2013, World Economic Forum: http://reports.weforum.org/global-risks-2013/.

Wo Sie uns finden

10719 Berlin
Kurfürstendamm 23
Tel: +49 (0)30 25468 01

01097 Dresden
Theresienstraße 29
Tel: +49 (0)351 81101 0

40476 Düsseldorf
Schwannstraße 6
Tel: +49 (0)211 8772 01

99084 Erfurt
Anger 81
Tel: +49 (0)361 65496 0

60486 Frankfurt am Main
Franklinstraße 50
Tel: +49 (0)69 75695 01
Consulting:
Franklinstraße 46–48
Tel: +49 (0)69 97137 0

06108 Halle (Saale)
Bornknechtstraße 5
Tel: +49 (0)345 2199 6

20354 Hamburg
Dammtorstraße 12
Tel: +49 (0)40 32080 0

30159 Hannover
Georgstraße 52
Tel: +49 (0)511 3023 0
Consulting:
Theaterstraße 15
Tel: +49 (0)511 93636 0

50672 Köln
Magnusstraße 11
Tel: +49 (0)221 97324 0

04317 Leipzig
Seemannstraße 8
Tel: +49 (0)341 992 7000

39104 Magdeburg
Hasselbachplatz 3
Tel: +49 (0)391 56873 0

68165 Mannheim
Reichskanzler-Müller-Straße 25
Tel: +49 (0)621 15901 0

81669 München
Rosenheimer Platz 4
Tel: +49 (0)89 29036 0

90482 Nürnberg
Business Tower
Ostendstraße 100
Tel: +49 (0)911 23074 0

70597 Stuttgart
Löffelstraße 42
Tel: +49 (0)711 16554 01

69190 Walldorf
Altrottstraße 31
Tel: +49 (0)6227 7332 60

Ihre Ansprechpartner

Für mehr Informationen

Peter Wirnsperger
Partner
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Dr. Andreas Knäbchen
Partner
Tel: +49 (0)89 29036 8582
aknaebchen@deloitte.de

Dr. Carsten Schinschel
Partner
Tel: +49 (0)211 8772 3163
cschinschel@deloitte.de

Dr. Claus Buhleier
Partner
Tel: +49 (0)69 75695 6523
cbuhleier@deloitte.de

Für weitere Informationen besuchen Sie unsere Website auf www.deloitte.com/de/cyber

Weitere Publikationen

- Cyber-Security – Die Perspektive des Informationsaustausches
- 2013 TMT Global Security Study
- Deloitte Consumer Review 2013 (UK)
- Exploring Strategic Risk 2013

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen und weder die Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited („DTTL"), noch eines der Mitgliedsunternehmen von DTTL oder ihre verbundenen Unternehmen (insgesamt das „Deloitte Netzwerk") erbringen mittels dieser Veröffentlichung professionelle Beratungs- oder Dienstleistungen.

Bevor Sie eine Entscheidung treffen oder Handlung vornehmen, die Auswirkungen auf Ihre Finanzen oder Ihre geschäftlichen Aktivitäten haben könnte, sollten Sie einen qualifizierten Berater aufsuchen. Keines der Mitgliedsunternehmen des Deloitte Netzwerks ist verantwortlich für Verluste jedweder Art, die irgendjemand im Vertrauen auf diese Veröffentlichung erlitten hat.

Deloitte erbringt Dienstleistungen aus den Bereichen Wirtschaftsprüfung, Steuerberatung, Consulting und Corporate Finance für Unternehmen und Institutionen aus allen Wirtschaftszweigen; Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Mit einem weltweiten Netzwerk von Mitgliedsgesellschaften in mehr als 150 Ländern verbindet Deloitte herausragende Kompetenz mit erstklassigen Leistungen und steht Kunden so bei der Bewältigung ihrer komplexen unternehmerischen Herausforderungen zur Seite. „To be the Standard of Excellence" – für rund 200.000 Mitarbeiter von Deloitte ist dies gemeinsame Vision und individueller Anspruch zugleich.

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited, eine „private company limited by guarantee" (Gesellschaft mit beschränkter Haftung nach britischem Recht), und/oder ihr Netzwerk von Mitgliedsunternehmen. Jedes dieser Mitgliedsunternehmen ist rechtlich selbstständig und unabhängig. Eine detaillierte Beschreibung der rechtlichen Struktur von Deloitte Touche Tohmatsu Limited und ihrer Mitgliedsunternehmen finden Sie auf www.deloitte.com/de/UeberUns.

© 2014 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

Stand 04/2014

FSC www.fsc.org
MIX
Papier aus verantwortungsvollen Quellen
FSC® C003486