Deloitte.

CFO Insights
Cyber-Security: Fünf grundlegende Wahrheiten

Cyber-Risiken scheinen allgegenwärtig zu sein. Datenpannen bei Einzelhändlern, Diebstahl von geistigem Eigentum – Systeme werden nahezu täglich gehackt und Daten gestohlen. Das Problem kann selbst den wackersten Chief Financial Officer (CFO) verunsichern – und das tut es oft auch.

Tatsächlich erscheinen Cyber-Angriffe in unserem vierteljährlichen CFO Signals™ Survey jetzt unweigerlich auf der Liste der Risiken, die CFOs am meisten beunruhigen. Die Liste umfasst unter anderem auch anhaltende makroökonomische Faktoren wie Konjunkturvolatilität und Überregulierung.[1] Als wir den Survey vor vier Jahren einführten, war das Cyber-Risiko noch kaum ein Thema. Heute wird es regelmäßig genannt. Auch in unseren CFO Transition Lab™ Sessions sprechen neu benannte CFOs über ihre zunehmende Sorge vor Cyber-Attacken.

Dieses neue Problembewusstsein hängt sowohl mit der Häufigkeit als auch mit den Kosten von Cyber-Angriffen zusammen. Laut der Studie „2014 Cost of Data Breach: Global Analysis" des Ponemon Institute belaufen sich die durchschnittlichen Gesamtkosten für eine Datenpanne jetzt weltweit auf 2,6 Millionen Euro. Dieser Wert liegt um 15% höher als im letzten Jahr und beträgt bei US-Unternehmen noch erheblich mehr, etwa 4,4 Millionen Euro. Darüber hinaus liegt laut dieser Studie die Wahrscheinlichkeit, dass ein Unternehmen in den kommenden 24 Monaten eine schwerwiegende Datenpanne mit 10.000 Datensätzen oder mehr erlebt, bei 22%.[2]

In Anbetracht der steigenden Kosten und der zunehmenden Professionalität von Cyber-Attacken konzentrieren sich CFOs verständlicherweise darauf, potenzielle Cyber-Risiken zu identifizieren und in ihren Unternehmen entsprechende Gegenmaßnahmen zu planen. Ein großer Teil der Finanzchefs ist zusätzlich für die IT verantwortlich und muss ebenfalls entscheiden, wie und wo Unternehmensressourcen in Präventionsmaßnahmen investiert werden sollen. In dieser Ausgabe von CFO Insights sprechen wir einige grundlegende „Wahrheiten" über Cyber-Security an und bieten praxiserprobte Vorschläge für das Investieren in einen unternehmensweiten Cyber-Security-Plan.

[1] „What's Keeping CFOs Up in 2014?" CFO Insights, Juni 2014; CFO Signals, Q2 2014; U.S. CFO Program, Deloitte LLP.

[2] „2014 Cost of Data Breach Study: Global Analysis", Ponemon Institute, Mai 2014.

Das bewegliche – und sich schnell ändernde – Ziel anvisieren

Das Cyber-Risiko in den Griff zu bekommen, kann für CFOs äußerst frustrierend sein, denn den Finanzchefs stehen oft keine Trendinformationen über die Schwächen in ihren Unternehmen zur Verfügung. Zudem werden klassische Sicherheitskontrollen (Firewalls, Virenschutzprogramme, Intrusion-Detection-Systeme [IDS], Intrusion-Prevention-Systeme [IPS] etc.) in Anbetracht der Allgegenwärtigkeit von Cyber-Risiken zunehmend weniger effektiv. Angreifer nutzen innovative Methoden, um diese Vorkehrungen zu umgehen (siehe Deloitte-Video „Companies like Yours“[3]).

Hinzukommt, dass das Schlachtfeld immer größer wird, unter anderem auch durch die Migration von Daten in die Cloud. Die potenziellen Einsparungen mögen attraktiv sein, aber der Wechsel in die Cloud bringt inhärente Sicherheitsfragen mit sich wie beispielsweise „Wer kann in der Cloud auf meine Daten zugreifen?“ und „Können meine Daten auch von anderen Kunden genutzt werden?“. Noch weiter verschärft wird das Problem durch die mobile Entwicklung. Neben den üblichen Desktop-Computern enthalten Notebooks und Smartphones in der Regel eine Fülle an persönlichen Informationen und eröffnen zahlreiche Zugriffsmöglichkeiten für Cyber-Crime. Last but not least sind diese Diebe geduldig: Cyber-Attacken waren auch in der Vergangenheit nicht unbedingt „Blitzangriffe“. Oft operieren Kriminelle über Monate und Jahre hinweg unter dem Sicherheitsradar einer Zielorganisation und schlagen dann im geeigneten Moment zu.

All das bedeutet, dass Unternehmen – und CFOs – einen langfristigen Kampf an mehreren Fronten führen, wobei die Erfolge schwer zu messen sind. Um im „Cyber-Krieg“ überhaupt eine Chance zu haben, müssen sich CFOs daher eine Reihe von Fakten vor Augen führen:

1. Ihr Unternehmensnetz wird kompromittiert werden

Es ist leider unumgänglich, dass Sie angegriffen werden. Als Betreiber eines Netzwerks werden Sie Risiken nie völlig vermeiden können. Stellen Sie sich dieser Tatsache.

2. Physische Sicherheit und Cyber-Security wachsen mehr zusammen

Physische Sicherheit wurde herkömmlicherweise meistens getrennt von der Cyber-Sicherheit betrachtet. Das ist nicht mehr der Fall, weil Bedrohungen wie Spionage, Diebstahl geistigen Eigentums, Betrug, Fälschung und Terrorismus zwar Verletzungen der Cyber-Sicherheit beinhalten können, möglicherweise jedoch auch mit einem physischen Zugriff beginnen – sei es durch Diebstahl von Zugangskonten oder die Kompromittierung von Rechnern von reisenden Mitarbeitern. In einem typischen Beispiel haben Administratoren vollständige Kontrolle über ein System wie eine Gehaltsliste, die Kundendatenbank oder die Abrechnungssysteme. Sie können ihre Zugriffsrechte nutzen, um gefälschte Rechnungen an sich selbst zu bezahlen, Darlehen zu besonderen Konditionen zu bewilligen oder Kreditkartendaten von Kunden sowie Mitarbeiterunterlagen mit vertraulichen Informationen zu kopieren. Diese Daten verkaufen sie weiter und begehen damit Identitätsdiebstahl, Veruntreuung oder andere Arten von Betrug.

3. Cyber-Schäden gehen weit über den finanziellen Verlust hinaus

Die durchschnittlichen Kosten einer Datenpanne sind gut dokumentiert. Hinzu kommen jedoch oft erhebliche langfristige Auswirkungen auf den Ruf und die Marke eines Unternehmens. Insbesondere bei Kundendaten können Datenpannen zu einem Vertrauensverlust führen, der sich unweigerlich auf den Umsatz auswirkt. Das ist ein Grund dafür, dass einige Zahlungsanbieter und auch das BKA die Nutzung neuer EC- und Kreditkarten fordern, bei denen Informationen auf Computerchips und nicht mehr wie bisher auf Magnetstreifen gespeichert sind.[4] Darüber hinaus erwägen viele Unternehmen jetzt den Abschluss einer Cyber-Versicherung, um mögliche Schäden zu begrenzen.

4. Nicht alles kann in gleichem Maße geschützt werden

Fragen Sie sich, was und wo die „Kronjuwelen“ Ihrer Organisation sind. Anders ausgedrückt: Welche Daten sind für den Betriebsablauf unerlässlich? Bei welchen Datenbanken könnte eine Kompromittierung Ihr Geschäft zum Erliegen bringen? Schließlich sind nicht alle Informationen in gleichem Maße schützenswürdig. Für einen Einzelhändler sind beispielsweise Kreditkartendaten von Kunden wesentlich, ebenso wie Informationen über die Logistik. In der Fertigungsindustrie sind es die Produktionsverfahren oder Informationen über Werkstoffe. Eine strukturierte Aufstellung von unternehmensspezifischen Daten-Clustern kann CFOs helfen, gezieltere Entscheidungen über die Priorisierung von Schutzmaßnahmen und andere Aspekte ihrer Cyber-Ausgaben zu treffen.

---

[3] „Companies like Yours“, Deloitte LLP, 2011. www.deloitte.com/de/cyber

[4] „MasterCard, Visa and American Express Propose New Global Standard to Make Online and Mobile Shopping Simpler and Safer“; Pressemitteilung, 1. Oktober 2013.

5. Ihre Schutzmauern sind wahrscheinlich hoch genug
Unternehmen investieren nach wie vor in großem Umfang in die klassischen Schutzmaßnahmen wie bessere Firewalls und Virenscanner. Tatsächlich reichen die meisten Schutzvorkehrungen vermutlich schon aus. Auf der anderen Seite sind Hacker höchstwahrscheinlich schon in Ihre Systeme eingedrungen, ohne dass sie entdeckt wurden. Unternehmen sollten sich daher deutlich mehr auf die Erkennung von Eindringungsversuchen konzentrieren, um Angriffe überhaupt erkennen und schnell auf den Vorfall reagieren zu können. Das genaue Verhältnis ist natürlich bei jedem Unternehmen anders, aber typischerweise werden von den IT-Ausgaben zum Schutz gegen Cyber-Risiken 30% für Schutzvorrichtungen, 50% für Erkennung und weitere 20% für die Erhöhung der Widerstandsfähigkeit aufgewandt.

Abb. 1 – Wie Cyber-Diebe angreifen

Vorfallkategorie	Prozentsatz
POS-Systemeinbrüche	14%
Web-App-Angriffe	35%
Missbrauch durch Insider	8%
Physischer Diebstahl/Verlust	<1%
Diverse Fehler	2%
Crimeware	4%
Karten-Skimmer	9%
DoS-Angriffe	<1%
Cyber-Spionage	22%
Alle Übrigen	6%

Häufigkeit der Vorfallkategorien bei 1.367 Datenpannen 2013.
Quelle: Verizon 2014 Data Breach Investigations Report

Die Grundsätze wirksamer Cyber-Risiko-Programme

Der Realität müssen Sie sich stellen, um einen wirksamen, unternehmensweiten Cyber-Risiko-Plan implementieren zu können. Folgende Punkte sollten Sie umsetzen:

Schaffen Sie unternehmensweit eine „Cyber-Sicherheits-Kultur"
In der gesamten Organisation müssen Bewusstsein, Aufklärung und Schulung gegeben sein, um das Cyber-Risiko zu bekämpfen. Sie mögen über erstklassige Hard- und Software verfügen, die Sie gegen Cyber-Angreifer schützt. Wenn jedoch nur ein nicht ausreichend geschulter Mitarbeiter einen E-Mail-Anhang mit Schadsoftware öffnet, können Ihre Systeme trotzdem völlig zum Erliegen kommen. Der Kampf gegen solche Risiken muss auf der obersten Ebene beginnen. Vorstand, Geschäftsführer und Finanzchefs legen die Governance und die Organisationsstruktur fest und sorgen dafür, dass alle Mitarbeiter sich ihrer tragenden Rolle bei der Abwehr von Cyber-Attacken bewusst sind.

Stellen Sie die richtigen Fragen an die richtigen Leute
Als CFO beziehen Sie Informationen über Cyber-Risiken hauptsächlich vom CIO, vom Chief Risk Officer (CRO) und vom Chief Information Security Officer (CISO). Die folgenden Fragen können den Dialog anregen:

- Wie identifizieren wir unsere kritischen Assets, die damit verbundenen Risiken und unsere Schwachstellen?
- Verfolgen wir, welche Informationen unsere Organisation verlassen und wo sie hinfließen?
- Wie wissen wir, wer sich wirklich in unser Netzwerk einloggt und von wo?
- Können wir die Informationen, die wir einem Cyber-Gegner mehr oder weniger freiwillig zugänglich machen, begrenzen?
- Decken unsere Sicherheitskontrollen das gesamte Unternehmen, einschließlich Zweigstellen und Tochterunternehmen?
- Verfügen wir über einen erprobten Incident-Response- und Krisenkommunikationsplan?

Führen Sie ein Cyber Security Framework ein
Im Februar veröffentlichte das NIST (National Institute of Standards and Technology) das „Framework for Improving Critical Infrastructure Cybersecurity Version 1.0".[5] Bei dessen Erstellung haben auch deutsche Unternehmen mitgewirkt. Dieses Rahmenwerk hatte US-Präsident Barrack Obama 2013 in seiner Rede zur Lage der Nation angekündigt. Es soll Unternehmen eine Reihe von Branchenstandards zur Verfügung stellen, um Cyber-Security-Risiken zu managen. Darin werden Hilfestellungen formuliert, wie Organisationen Cyber-Gefahren identifizieren, sich dagegen schützen, ihr Auftreten erkennen, darauf reagieren und sich davon erholen können. Das Framework soll künftig eine Grundlage für bewährte Verfahren bilden, die Unternehmen nutzen können, um beispielsweise rechtliche Risiken im Zusammenhang mit Cyber-Bedrohungen zu bewerten, indem es u.a. die verstärkte Mitwirkung des Vorstands bei der Beaufsichtigung von Cyber-Security-Risiken und die Einführung von Regelungen zum Informationsaustausch fördert. Wird dieses Rahmenwerk andererseits nicht ausreichend umgesetzt, werden eventuell für Sektoren mit kritischen Infrastrukturen noch zusätzliche regulatorische Anforderungen empfohlen.

In Deutschland wird das neue Sicherheitsgesetz umfassende Anforderungen an Unternehmen stellen, wie bspw. die Meldepflicht von Vorfällen für ausgewählte Sektoren oder auch der Nachweis, dass geeignete Sicherheitsmaßnahmen umgesetzt wurden. Auf der Basis des NIST-Rahmenwerks, den Vorgaben der ISO 27001 oder den Empfehlungen des BSI können Unternehmen geeignete Managementstrukturen für die Sicherheit schaffen.

Benennen Sie einen Verantwortlichen
Ein von einigen Unternehmen angewandtes bewährtes Verfahren ist es, mit der Beobachtung und Ermittlung von Cyber-Risiken einen internen Mitarbeiter zu beauftragen. Dieser hat die Aufgabe, über auftretende Datenpannen nicht nur aus Datenschutzgesichtspunkten zu ermitteln und sie an die zuständigen Stellen zu melden. Dem Cyber-Verantwortlichen untersteht zwar nicht der gesamte Sicherheitsbereich, aber sie oder er kann die „Sprachbarriere" zwischen den Cyber-Experten und der Unternehmensführung überbrücken. In einigen Unternehmen obliegt es beispielsweise dem CIO, für angemessene Schutzvorkehrungen zu sorgen. Für Beobachtung oder Erkennung ist jedoch ein Mitglied des CRO-Teams zuständig, das an den CFO berichtet.

Informieren Sie sich
Als CFO müssen Sie über Cyber-Risiken informiert sein. Sie können sich nicht ausschließlich auf Ihren CIO, CISO oder Ihren benannten „Cyber-Verantwortlichen" verlassen. Dazu ist aber mehr notwendig als die Teilnahme an einem Online-Kurs oder die Lektüre eines der unendlich vielen Bücher über Cyber-Security, die inzwischen erhältlich sind. Sie müssen sich direkt und auf praktischer Basis mit Cyber-Gefahren vertraut machen, indem Sie die Risiken Ihres Unternehmens abbilden und dann das Was und Wie der Sicherheit untersuchen.

Testen Sie die Security-Pläne
Im Rahmen von Cyber-Simulationsübungen können Teilnehmer sich in Echtzeit als „gute" und „böse" Gegner auseinandersetzen. Sie haben die Möglichkeit, sich rasch mit den Risiken vertraut zu machen, herauszufinden, wo die wichtigsten Assets der Organisation angesiedelt sind, und Lösungen für die Prävention zu identifizieren.

Erreichen eines Comfort-Levels

Unternehmen sind kontinuierlich dem Risiko von Cyber-Angriffen ausgesetzt – eine Bedrohung, die nicht ignoriert werden kann. Das Verständnis dieser Sachverhalte und die Umsetzung geeigneter Maßnahmen gewähren CFOs zwar keine absolute Sicherheit, aber immerhin die Gewissheit, dass innerhalb ihrer Risikotoleranzgrenzen Maßnahmen zum Schutz und zur Erkennung ergriffen wurden. Es liegt in der Natur der Cyber-Security, dass keine Lösung alle Risiken vollständig abdecken kann. Die Umsetzung eines unternehmensweiten Cyber-Security-Plans gestattet CFOs jedoch ein Mindestmaß an Sicherheit.

[5] Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, National Institute of Standards and Technology, Februar 2014.

Cyber-Security-Checkliste

Sie können Schritt für Schritt das Risiko eines Cyber-Angriffs verringern. Tatsächlich reduzierten laut der Studie „2014 Cost of Data Breach: Global Analysis" des Ponemon Institute eine starke Sicherheitskultur, ein Incident-Response-Plan und die Benennung eines Chief Information Security Officer die Kosten einer Datenpanne jeweils um 14,14 US-Dollar, 12,77 US-Dollar und 6,59 US-Dollar pro Datensatz.[6] Zusätzlich können die folgenden Maßnahmen CFOs eine Anleitung für die Umsetzung eines unternehmensweiten Cyber-Security-Plans bieten:

1. Bewerten Sie den bestehenden Cyber-Incident-Response-Plan

Konzentrieren Sie sich auf die Schutzmaßnahmen im Hinblick auf Ihre „Kronjuwelen" und darauf, wie Sie auf einen Vorfall reagieren würden. Das hierfür verantwortliche Team sollte leitende Führungskräfte sowohl aus den Geschäftsbereichen als auch aus dem Backoffice und der Verwaltung umfassen.

2. Identifizieren Sie, welche Rolle Finanzen bei der Cyber-Security spielen

Arbeiten Sie mit Ihrem CIO und mit Ihren Führungskräften zusammen, um herauszufinden, wie der Finanzbereich zur Schaffung der nötigen Sicherheits- und Informationsschutzkultur beitragen kann. Organisationen können ihre Sicherheitsvorkehrungen verbessern, indem sie Cyber-Security sowie dem Schutz von Informationen den richtigen Wert beimessen. Denken Sie daran: „Sicherheit beginnt mit mir selbst."

3. Fordern Sie regelmäßige Berichte über Sicherheitsrisiken

Diese Berichte sollten von leitenden Führungskräften erstellt werden und auf Informationsschutz- und Sicherheitsrisiken, beruhend auf spezifischen Risikoindikatoren, abstellen anstatt auf den Projektstatus von neu eingeführten Maßnahmen.

4. Überprüfen Sie das Cyber-Security-Budget

Oft haben Sicherheitsbudgets eine niedrigere Priorität als andere IT- oder geschäftsrelevante Investitionen. Infolgedessen sind Unternehmen nicht optimal auf den Umgang mit Risiken und Angriffen vorbereitet. Es empfiehlt sich, das Budget für die Cyber-Sicherheit jährlich zu überprüfen. Und sollten Sie das Budget gar reduzieren wollen, überlegen Sie sich das bitte mindestens zweimal.

5. Fassen Sie den Abschluss einer Cyber-Versicherung ins Auge

Nutzen und Notwendigkeit einer solchen sollten ebenfalls jährlich neu bewertet werden.

---

[6] „2014 Cost of Data Breach Study: Global Analysis", Ponemon Institute, Mai 2014.

Ihr 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 8528
aknaebchen@deloitte.de

Peter Kestner
Partner
Tel: +49 (0)89 29036 8064
pkestner@deloitte.de

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

Stand 08/2014