TOLERANZ FÜR VERÄNDERUNG

Um zu verstehen, wie umfassend Unternehmen für das Haifischbecken gerüstet sind, muss abschließend evaluiert werden, wie gut sie mit Veränderungen in der Informationstechnologie umgehen. Wie bereits in diesem Paper erläutert wurde, stellen Best Practices für Cyber-Sicherheit eine Abkehr von Standardverfahren dar, die sich im Laufe der Jahrzehnte entwickelt haben. Sollen Mentalität und Philosophie im Bereich der Sicherheit verändert werden, ist es wichtig, dass Unternehmen Veränderungen der zugrundeliegenden Informationstechnologie nutzen.

Die digitale Transformation ist ein perfektes Beispiel dafür. Sie ist einer der Hauptfaktoren, der Unternehmen dazu zwingt, im Haifischbecken zu schwimmen. Der Standardansatz von Sicherheitsverantwortlichen wäre wahrscheinlich, die Anwendung neuer Technologien wie Social Business, Mobility, Big Data/Analytik und Cloud-Computing zu verhindern. Denn durch sie steigen die Risiken. Das ist jedoch keine ausgereifte Herangehensweise. Innovative Unternehmen dürfen die digitale Transformation nicht blockieren, sondern müssen Benutzern die nötigen Tools zur sicheren Umsetzung der digitalen Transformation bereitstellen.

In Abbildung 4 wird aufgezeigt, dass der Reifegrad einer Organisation gemäß der in dieser Studie verwendeten Definition ein Indikator dafür ist, wie gut Unternehmen mit IT-Veränderungen umgehen. Unternehmen mit dem niedrigsten Reifegrad haben für gewöhnlich mit IT-Veränderungen Probleme oder finden es zumindest schwierig, komplexe Maßnahmen umzusetzen. Doch je höher der Reifegrad, umso wahrscheinlicher ist es, dass Unternehmen gut mit diesen Veränderungen zurechtzukommen oder die Bereitstellung sogar „sehr gut“ bewältigen.

Diese Ergebnisse zeigen, dass der Schlüssel zu einem erfolgreichen, dynamischen Unternehmen im Kontext von Cyber-Security in einem ausgereiften Sicherheitsansatz und der Nutzung (statt der Abwehr) von IT-Veränderungen liegt. Das gilt auch umgekehrt, denn ein Thema spiegelt das andere wider. Damit IT-Veränderungen umgesetzt werden können, muss ein Unternehmen die Auswirkungen auf die Sicherheit genau nachvollziehen können. Gleichzeitig ist es für einen ausgereiften Sicherheitsansatz wichtig, dass die erforderlichen Änderungen der IT umgesetzt werden können.

Fähigkeit zur Bewältigung von Veränderungen nach Cyber-Risiko-Reifegraden

Q2. Welche Aussage spiegelt die Fähigkeiten Ihrer IT-Abteilung in Bezug auf Geschäftsanforderungen für neue oder erweiterte Anwendungen oder Dienste am besten wider?

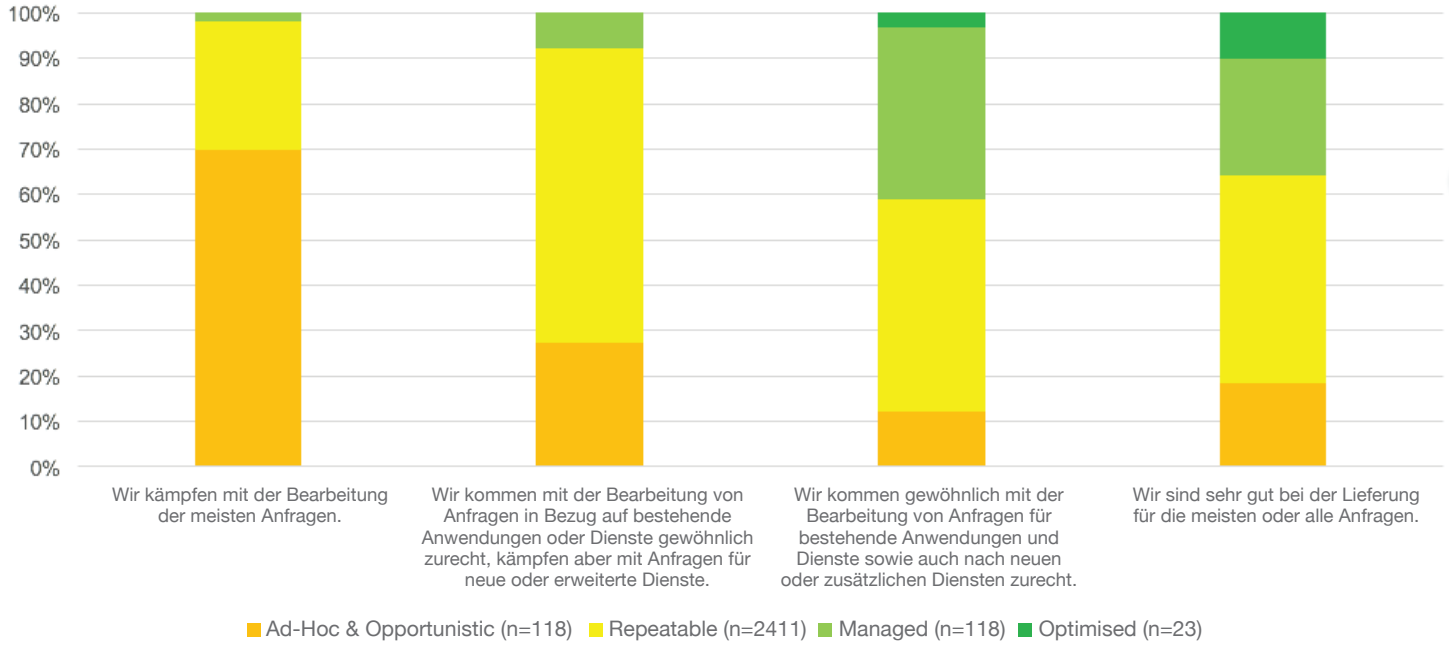

Abbildung 4 *Source: IDC, 2016*

10 EMPFEHLUNGEN FÜR IHR UNTERNEHMEN

Im Folgenden finden Sie zehn Empfehlungen, die als Leitfaden für die Verbesserung des Sicherheitsreifegrads in Ihrem Unternehmen verwendet werden können.

- **Vergleichen Sie Ihre Situation mit Unternehmen, die hinsichtlich Branche, Größe und geografischer Präsenz vergleichbar sind.**
- **Stärker Sie Ihre eigene Motivation voranzukommen und legen Sie fest, welchen Reifegrad Sie anstreben.**
- **Ermitteln Sie Lücken zwischen Ihrem derzeitigen Sicherheitsansatz und dem angestrebten Security-Level.**
- **Ziehen Sie externe Sicherheitsspezialisten für die Entwicklung und Umsetzung erforderlicher Änderungen in Betracht, die zur Erreichung Ihres Ziels notwendig sind.**
- **Finden Sie heraus, welche Sicherheitsprozesse und -aktivitäten kritisch und welche weniger kritisch und repetitiv sind.**
- **Überlegen Sie, welche eher unkritischen Aktivitäten automatisiert werden können, um Ressourcen einzusparen.**
- **Prüfen Sie, inwiefern die Ergebnisse durch die Zusammenarbeit mit MSS-Anbietern verbessert werden könnten. Am besten beginnen Sie mit weniger kritischen Aktivitäten und nutzen globale und industrialisierte Bereitstellungsmodelle.**
- **MSS werden sich immer stärker zu Commodity entwickeln. Ziehen Sie jedoch auch spezialisierte Dienstleistungen in Betracht, die die gewünschten Ergebnisse hinsichtlich einer Kostensenkung oder Qualitätsverbesserung erzielen könnten.**
- **Verwenden Sie einen risikobasierten Sicherheitsansatz, der das gesamte Unternehmen umfasst. Alle Benutzer stellen potenziell eine „Bedrohung von innen“ dar. Deshalb benötigen Sie eine ganzheitliche Sicherheitskultur und -strategie.**
- **Beziehen Sie Sicherheitsbeauftragte von Anfang an in neue Geschäftsinitiativen mit ein. Wenn Sie schon in der Entwicklungsphase für die Sicherheit neuer Initiativen sorgen, haben Sie später weniger Probleme.**