# SCHWIMMEN IM HAIFISCHBECKEN

IDC Analyze the Future

## Evaluation von Sicherheit und Best Practices im Vergleich zu ähnlichen Unternehmen

### EINLEITUNG

Die Leitung eines Unternehmens im 21. Jahrhundert gleicht einem Tauchgang im Haifischbecken. Die Gefahren sind offensichtlich: Angreifer werden von Tag zu Tag fähiger, organisierter und arbeiten besser zusammen. Trotzdem müssen Sie die digitale Transformation meistern – heute ein unternehmenskritisches Thema für CEOs. Das heißt, dass Sie immer tiefer in das Haifischbecken vordringen müssen.

Mit den Technologien der digitalen Transformation – Big Data/Analytics, Cloud Computing, Mobility und Social Business – werden Unternehmensanwendungen und -daten außerhalb des sicheren Perimeters von Endgeräten oder Netzwerk genutzt. Das bedeutet geringere Transparenz und erschwerte Kontrolle für die Sicherheitsverantwortlichen. Sie befinden sich also nicht nur in trüben Gewässern; auch die Tür des Käfigs, der Sie bisher vor den Haien geschützt hat, ist mittlerweile weit geöffnet.

Die digitale Transformation zu ignorieren ist keine Option. Welch desaströse Auswirkungen dies hätte, sieht man an Unternehmen wie Blockbusters (DVD-Verlieh) und Borders (Buchhandel), die es nicht geschafft haben, sich an die neue Realität anzupassen und die Konsequenzen zu verstehen. Vielmehr ist ein grundlegend neuer technologischer Ansatz und eine neue strategische Denkweise erforderlich. In diesem Whitepaper werden Best Practices solcher Unternehmen erläutert, deren Sicherheitsansatz einen sehr hohen Reifegrad erreicht hat. Wenn Sie im Haifischbecken schwimmen und vielleicht sogar zurückbeißen möchten, benötigen Sie eine neue Perspektive.

### VERWENDUNG DIESES WHITEPAPERS

Dieser Bericht soll Ihnen Informationen über die Merkmale und die unterschiedlichen Reifegrade bezogen auf IT-Sicherheit liefern. Er enthält Beispiele für Best Practices für die Erhöhung der Sicherheit in Ihrem Unternehmen. Außerdem werden Innovationsbeschleuniger benannt, die eine besonders positive Wirkung auf die Sicherheit haben. Abschließend erhalten Sie Empfehlungen zur Verbesserung Ihrer Position im Vergleich zu vergleichbaren Unternehmen. Das vorliegende Paper basiert auf einer Studie aus dem Sommer 2016, für die 500 leitende Entscheidungsträger im Sicherheitsbereich aus Frankreich, Deutschland, Italien, Spanien und Großbritannien befragt wurden.

# SICHERHEITSREIFEGRAD VERGLEICHBARER UNTERNEHMEN

Auf Grundlage unserer Befragung von 500 leitenden Entscheidungsträgern für IT-Security konnten wir unterschiedliche Reifegrade identifizieren. In aufsteigender Reihenfolge sind das die folgenden fünf Reifegrade:

**ad-hoc**
**opportunistisch**
**wiederholbar**
**gesteuert**
**optimiert**.

Die Verteilung der Unternehmen auf die fünf Reifegradstufen gleicht für gewöhnlich einer klassischen „Glockenkurve“ (Normalverteilung) wie in Abbildung 1.

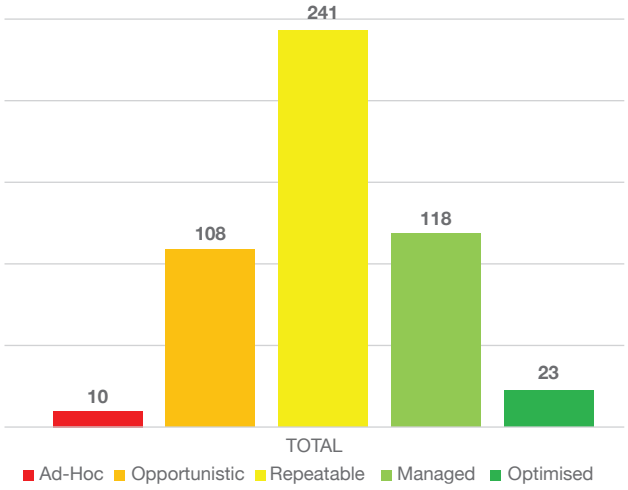


**Abbildung 1**

*Source: IDC, 2016*

Die Abbildung zeigt, dass es nur sehr wenige Unternehmen innerhalb der betrachteten Peergroup gibt, die einen sehr niedrigen oder einen sehr hohen Reifegrad aufweisen. Der Großteil befindet sich mehr oder weniger in der Mitte. Wenn Sie sicher im Haifischbecken schwimmen möchten, sollten Sie nicht nur mit den anderen Unternehmen gleichziehen, sondern bewährte Verfahren anwenden. Im nächsten Abschnitt wird erklärt, wie Best Practices im Sicherheitsbereich aussehen.

# BEST PRACTICES ZUR GEWÄHRLEISTUNG EINER HOHEN SICHERHEIT

In der Vergangenheit zielten Sicherheitstechnologien darauf ab, Unternehmen vor bekannten Bedrohungen zu schützen. Da Geräte, Anwendungen und Daten hinter einer Firewall verwendet wurden, konnten die Bedrohungen für Endgeräte und Netzwerk mit Perimeterkontrollen eingedämmt werden. Es gibt jedoch zwei Trends, aufgrund derer derartige vorbeugende Sicherheitsmodelle nicht mehr ausreichen:

- Erstens werden Unternehmensanwendungen und -daten aufgrund der digitalen Transformation vermehrt auch außerhalb des Perimeters und außerhalb der Kontrolle von internen Sicherheitsteams verwendet.
- Zweitens haben die Bedrohungen ein noch nie dagewesenes Ausmaß erreicht. Jeden Tag tauchen mehr als eine Million neue Malware-Varianten auf und es ist einfach unmöglich, schnell genug Signaturen zu entwickeln, um herkömmliche Schutzmaßnahmen zur Blockierung neuer Bedrohungen aufrechtzuerhalten.

Es sind zwingend neue Ansätze erforderlich, die Unternehmen helfen, unbekannte Bedrohungen zu identifizieren und zu bekämpfen sowie bekannte Bedrohungen zu blockieren. Es reicht nicht mehr aus, abzuwarten bis ein Angriff festgestellt wird. Vielmehr muss proaktiv nach Hinweisen für eine potenzielle Beeinträchtigung der Sicherheit gesucht werden. Dieser Ansatz erfordert jedoch einen Perspektivwechsel im Hinblick auf die Sicherheitsstrategie. Hierfür ist es hilfreich zu analysieren, was die Effektivität der Sicherheitsmaßnahmen über alle Reifegrade hinweg einschränkt (siehe Abbildung 2).

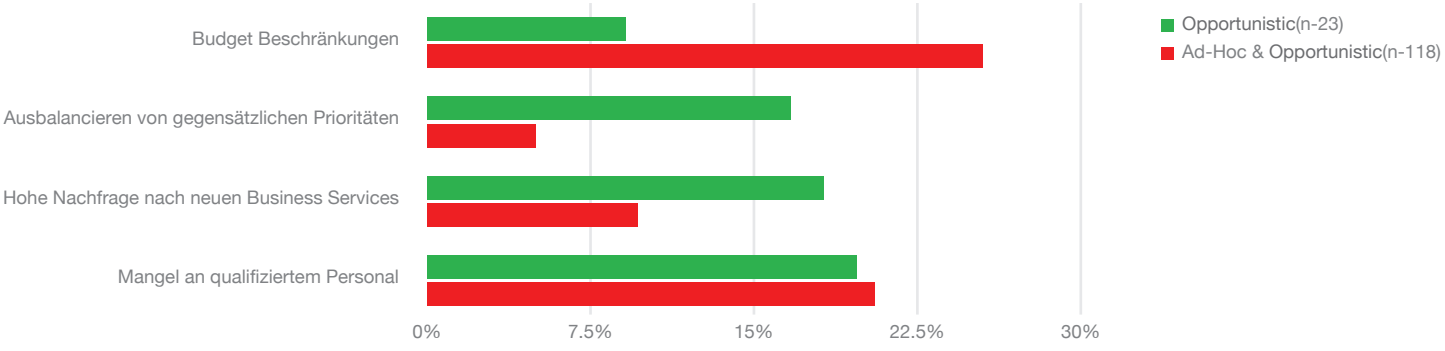


**Abbildung 2**

*Source: IDC, 2016*

Es gibt bestimmte Probleme, die alle Unternehmen betreffen, egal welchen Reifegrad sie vorweisen. Alle Unternehmen leiden unter Kostendruck und einem Mangel an qualifizierten Arbeitskräften. Angesichts des globalen Fachkräftemangels im Sicherheitsbereich ist dies nicht überraschend. Aufschlussreicher sind jedoch Informationen darüber, inwiefern darüber hinaus Probleme mit Best Practices angegangen werden können.

Bei Unternehmen mit niedrigerem Reifegrad sind der Kostendruck und der Fachkräftemangel die größten Probleme. Bei Unternehmen mit höherem Reifegrad sind diese Probleme jedoch gleichbedeutend mit anderen Herausforderungen, wie zum Beispiel dem Management miteinander in Konflikt stehender Prioritäten und die Absicherung neuer Geschäftsbereiche. Hier muss ein großes Umdenken stattfinden: Für IT-Security gehört es zu den Best Practices, die Geschäftsanforderungen der Unternehmen zu berücksichtigen.

Sobald der Perspektivwechsel stattgefunden hat, sollten Unternehmen bedenken, was das für die praktischen Sicherheitsansätze bedeutet. Besonders wichtig ist ein Übergang von reaktiven Sicherheitsmodellen zu einer proaktiven Gewährleistung der IT-Sicherheit. Wie in Abbildung 3 verdeutlicht wird, gibt es zwei eindeutige Trends über alle Reifegrade hinweg. Je höher der Reifegrad in einem Unternehmen, umso unwahrscheinlicher ist es, dass Unternehmen auf proaktive Sicherheitsmaßnahmen verzichten. Es ist vielmehr davon auszugehen, dass diese bereits geplant oder verwendet werden.

**Anwendung proaktiver Sicherheitsmaßnahmen nach Reifegrad**

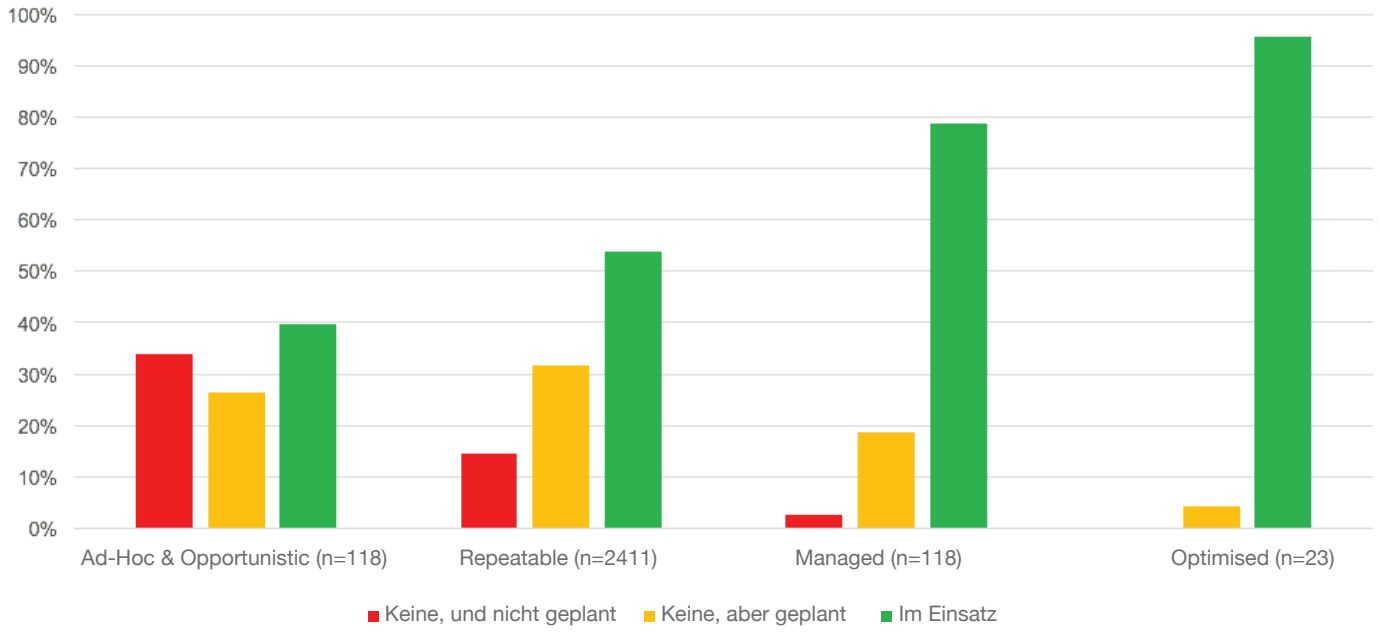


**Abbildung 3**

*Source: IDC, 2016*

Ergebnisse unserer Studie zeigen, dass Unternehmen Sicherheitstechnologien wie Bedrohungsanalysen, künstliche Intelligenz und heuristische Analysen von Benutzerverhalten anwenden, um diese proaktiven Ansätze umzusetzen. Ähnlich wie bei den proaktiven Sicherheitsmaßnahmen wird es umso wahrscheinlicher, dass Lösungen wie künstliche Intelligenz und Heuristik Anwendung finden, je fortschrittlicher der Sicherheitsansatz eines Unternehmens ist.

Obwohl proaktive Sicherheitsansätze eine Chance für die Verbesserung der Sicherheit bieten, sind sie auch mit Herausforderungen verbunden. Proaktive Methoden erfordern zum Beispiel die Erfassung und Überwachung operativer und verhaltensbezogener Log- und Protokolldateien in viel größerem Umfang. Da die finanziellen Ressourcen von Sicherheitsteams knapp sind, muss eine nüchterne Diskussion darüber geführt werden, mit welchen Methoden interne Ressourcen entlastet werden können. Die Best Practices zeigen zwei mögliche Lösungen auf.

## OUTSOURCING

Obwohl die Gewährleistung der Unternehmenssicherheit eine schwierige Aufgabe darstellt, sind im Allgemeinen interne Teams dafür verantwortlich. Dafür gibt es viele gute Gründe. Erstens gilt Sicherheit als unternehmenskritisch. Durch Outsourcing steigt die Gefahr, dass interne Teams einen schlechteren Überblick und weniger Kontrolle über die Sicherheitslage haben. Anbieter von Managed Security Services (MSS) haben in der Vergangenheit vollmundige Versprechen gemacht, konnten diese in der Praxis jedoch nicht immer einlösen. Zweitens kann die Entscheidung für ein Outsourcing so ausgelegt werden, dass interne Teams ihren Misserfolg eingestehen und zugeben, dass sie die Arbeit nicht alleine bewältigen können.

In einer vernetzten Welt agiert jedoch kein Unternehmen völlig losgelöst und ist somit auch nicht immun gegen Bedrohungen. Dies gilt insbesondere dann, wenn europäische Unternehmen beschränkte Sicherheitsressourcen haben und externe Security-Dienstleister aufgrund globaler Reichweite, industrialisierter Bereitstellungsmodellen und besserem Zugang zu qualifiziertem Personal immer besser aufgestellt sind, um den erforderlichen Support bieten zu können. Deshalb sollten jene, die Best Practices im Sicherheitsbereich anwenden möchten, unbedingt MSS in Betracht ziehen.

MSS können Unternehmen zwar helfen, den Druck auf interne Ressourcen zu verringern, sie dürfen aber nicht die einzige Maßnahme darstellen. IDC Research zeigt, dass es am besten ist, nicht alle Aufgaben outzusourcen. Vielmehr sollte eine Balance zwischen interner Bereitstellung und MSS gefunden werden, die einerseits die geschäftlichen Anforderungen erfüllt und andererseits der Risikobereitschaft des Unternehmens entspricht. Zudem ist es wichtig, qualifizierte Sicherheitsfachkräfte im Unternehmen zu halten, damit nachvollzogen werden kann, welche strategischen Auswirkungen geschäftliche Entscheidungen auf die Sicherheit haben – und umgekehrt. Da die Gewährleistung von Sicherheit immer mehr durch das Risikomanagement getrieben und als unternehmensweite Aufgabe begriffen wird, handelt es sich hierbei um ein entscheidendes Merkmal von Best Practices für die Unternehmensführung und die Sicherheit.

## AUTOMATISIERUNG

Neben MMS gibt es eine weitere wichtige Maßnahme, die Unternehmen angesichts der Ressourcenknappheit und dem Ungleichgewicht zwischen digitaler Transformation und neuen Bedrohungen ergreifen können: die Automatisierung. Automatisierung ermöglicht das Management und die Umsetzung von Maßnahmen auf Basis entsprechender Security-Produkte. Das Einbeziehen interner Mitarbeiter hilft dabei den Überblick und die Kontrolle über die Sicherheit beizubehalten.

Das fördert den Einsatz von künstlicher Intelligenz und Cognitive Computing im Sicherheitsbereich, um die interne Ressourcen weiter zu entlasten und Maschinen Entscheidungen zu übertragen. Eines ist jedoch klar: zu den Best Practices gehört auch (zumindest vorläufig) einen gewissen Grad an menschlicher Kontrolle beizubehalten, um einen reibungslosen automatisierten Betrieb gewährleisten zu können und gerade die kritischsten Entscheidungen nicht in die Hände von Robotern zu legen.