Sicher im Cyberspace

Reifegradbestimmung und Handlungsempfehlungen auf Basis des Cyber Security Maturity Assessments

Immer öfter sind Unternehmen mit zunehmend aggressiven und raffinierten Cyberangriffen konfrontiert. Wer nicht angemessen vorbeugt und Vorfälle adäquat verfolgt, handelt unternehmerisch leichtfertig. Das Cyber Security Maturity Assessment von KPMG unterstützt Sie bei der fähigkeitsgradbezogenen Bewertung Ihrer Sicherungsmaßnahmen.

Die Herausforderung

Daten und Informationen sind ein immer stärkerer Faktor für den Unternehmenserfolg. Zunehmend schwierig jedoch wird ihr adäquater und kosteneffizienter Schutz. Dies liegt an Veränderungen der betreffenden Infrastruktur, wie beispielsweise durch Cloud und Mobile Computing, und an enger vernetzten Geschäftsprozessen durch die technische Transformation. Vor allem aber liegt es an einer gestiegenen Bedrohung durch Cyberattacken.

Für den individuell passenden Schutz müssen Unternehmen gezielte Vorkehrungen treffen und technische wie prozessuale Maßnahmen sinnvoll kombinieren. Diese Aufgabe ist nicht zuletzt deshalb sehr komplex, da Angreifer verschiedene Ziele verfolgen und ihre Attacken entsprechend unterschiedliche Folgen nach sich ziehen können.

Unsere Leistung

Das Cyber Security Maturity Assessment (CSMA), eine webbasierte Anwendung von KPMG, veranschaulicht Ihnen schnell und systematisch, wie es im Detail um die Cybersicherheit Ihres Unternehmens bestellt ist und in welchen Bereichen Sie handeln sollten.

Grundlage des CSMA bildet unsere langjährige Erfahrung mit Cyber Security- und IT-Forensik-Projekten. Zudem orientieren wir uns an den Best Practice-Anforderungen international anerkannter Normen (ISO 27001:2013, NIST, SANS 20 Critical Security Controls etc.).

Die Analyse erfasst alle relevanten Bereiche mit zahlreichen Themenfeldern:

Cybersicherheitsmanagement

- Ziele
- Rollen und Zuständigkeiten
- Ressourcen
- Risikomanagement
- Überprüfungen und Verbesserungen
- Dokumentenmanagement
- Aufzeichnungs- und Nachweismanagement

Organisatorisches

- Sicherheit in Personalprozessen
- Umgang mit Drittparteien
- Kennzeichnung von und Umgang mit Informationen
- Cyber Security Incident Management
- Business Continuity Management
- Compliance

Technisches

- Physische Sicherheit
- IT-System- und Anwendungssicherheit
- Netzwerksicherheit
- Überwachung und Protokollierung
- Vulnerability Management
- Kryptografie
- Mobile Computing
- Changemanagement

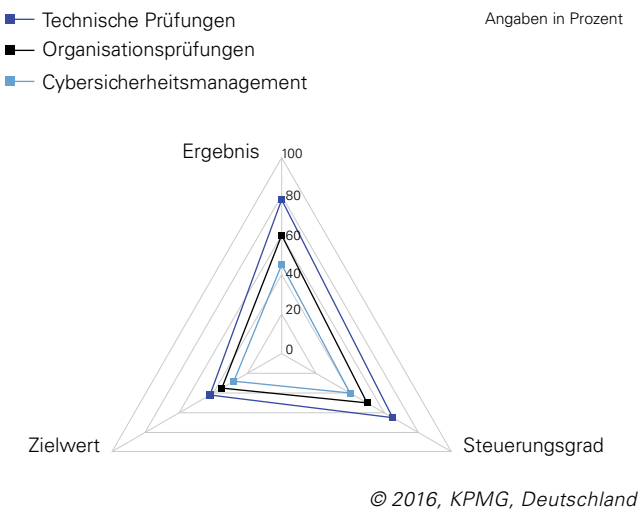
– Identitäts- und Zugangskontrolle
– Anschaffung, Entwicklung und Wartung von Systemen
– IT-forensische Analysen

Das Analysemodell ist so konzipiert, dass auch die unterschiedlichen Motivationen Ihrer möglichen Angreifer und die potenziellen Folgen von Cyberattacken für Ihr Unternehmen einbezogen werden. Die folgende Grafik veranschaulicht dies:

Angreifer im Cyberspace	
„Hacktivisten“ Ideologisch inspiriert – Motivation: neue Loyalitäten – dynamisch, flexibel – Folgen: öffentliche Aufmerksamkeit, Reputationsschäden	Organisiertes Verbrechen Global, schwierig aufzuspüren und zu belangen – Motivation: finanzieller Vorteil – Folgen: Datenverluste, Informationseinbußen
Insider Teils individuelle Motive, teils auch versehentlich – Motivation: Unzufriedenheit, Neid, finanzieller Vorteil – Folgen: Betriebsstörungen, Informationseinbußen, Reputationsschäden	Politische Einheiten Spionage oder Sabotage – Motivation: politischer, wirtschaftlicher oder militärischer Vorteil – Folgen: Betriebsstörungen, Zerstörungen, Daten- und Informationsverluste, Reputationsschäden

Die Ergebnisse des CSMA, die Ihnen in kürzester Zeit umfassende Erkenntnisse zur Beschaffenheit Ihrer Cybersicherheit und zu eventuellem Handlungsbedarf ermöglichen, werden in Form standardisierter systematischer Daten präsentiert.

Beurteilung eines Unternehmens mit dem Cyber Security Maturity Assessment (Beispiel)



Mit Abschluss des CSMA erhalten Sie neben den Daten zu den abgefragten Bereichen auch Informationen dazu, wie vergleichbare Unternehmen bei diesen Aspekten vorgehen. Darüber hinaus entwickeln wir – gestützt auf die genannten Angaben – Empfehlungen für ein individuelles Cybersicherheitskonzept Ihres Unternehmens.

Bestens für Sie aufgestellt

Auch im Bereich Cybersicherheit und Forensic gehört KPMG zu den führenden Anbietern. Unser weltweites Netzwerk mit über hundert Spezialisten allein in Deutschland sichert Ihnen höchste Vertraulichkeit und Integrität zu.

Sprechen Sie uns an! Unsere Cyberexperten unterstützen Sie.

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft

Uwe Bernd-Striebeck
Partner, Head of Cyber Security
T +49 201 455-6870
uberndstriebeck@kpmg.com

Hans-Peter Fischer
Partner, Cyber Security
T +49 69 9587-2404
hpfischer@kpmg.com

www.kpmg.de

www.kpmg.de/socialmedia