Wie gehen Sie mit dem Thema Cyber-Security um?

Informationssicherheit ist Chefsache

Sind Sie sicher, dass Sie als Entscheider das Thema Cyber-Security in Ihrem Unternehmen optimal handhaben? Sollten Sie die meisten unserer folgenden Experten-Fragen mit „Nein“ beantworten, gehören Strategie und Strukturen auf den Prüfstand. Anregungen zum Thema gibt Arne Helemann, Experte für strategische Informationssicherheit bei TÜV Rheinland.

Frage 1: Bewerten Sie regelmäßig das Bedrohungspotenzial für Ihre Organisation in Bezug auf Cyber-Attacken? Bei vielen Unternehmen ist das nicht der Fall. Neuartige Bedrohungen, wie gezielte komplexe Angriffe, bei denen herkömmliche, signaturbasierte Lösungen nicht funktionieren und die völlig andere Abwehrstrategien erfordern, haben Organisationen oft gar nicht auf dem Radar – weil personelle Ressourcen oder Know-how fehlen.

Frage 2: Ihr Unternehmen betreibt verschiedene Management-Systeme, wie zum Beispiel ISMS, QMS, BCMS. Findet eine angemessene Abstimmung zwischen den Managementsystemen, Fachbereichen, Kernprozessen und den wesentlichen Unterstützungsprozessen statt? Fehlt dieses Zusammenspiel, dann sollten Sie prüfen lassen, ob Maßnahmen der IT Security unnötig Ressourcen verschwenden, weil eine zentrale Implementierung fehlt oder sich Maßnahmen gar gegenseitig kannibalisieren. Dies kann nicht im Sinne des Unternehmens sein.

Frage 3: Pflegen Sie eine offene Unternehmenskultur? Die gelebte Kultur ist die Basis für das Handeln der Mitarbeiter. Häufig passiert es, dass Cyber-Security-Risiken vor dem Management systematisch kleingeredet werden und das Risikomanagement im Unternehmen nicht mehr ist als ein Feigenblatt. Das kann zu Fehleinschätzungen in der Identifikation, Analyse und Bewertung der Cyber-Risiken führen und zu einer nicht zielgerichteten, wirtschaftlich nicht angemessenen Risikobehandlung.

Frage 4: Sind Verantwortlichkeiten für die in Produktionsanlagen, Steuerungssystemen oder auch Multifunktionsgeräten vorhandenen IT-Schnittstellen in Fachbereichen verankert, die über eine ausreichende Expertise verfügen, um

Arne Helemann
Experte für strategische Informationssicherheit, TÜV Rheinland

die IT-Schnittstellen im Gesamtkontext angemessen und sicher zu betreiben? Diese Schnittstellen sind mögliche Ursache für eine höhere Verwundbarkeit gegenüber Cyber-Attacken. Schwachstellen bei der Integration in die bestehende IT, unangemessene Benutzerauthentifizierung oder mangelhaftes Patchmanagement sind typische Symptome eines solchen Problems.

Frage 5: Ist Informationssicherheit für Sie eine Management-Aufgabe oder eine Teildisziplin Ihrer IT? Findet Ihr CISO bei der Geschäftsführung ein offenes Ohr? Für viele Top-Entscheider ist es vielfach schwer verständlich, dass das Thema Informationssicherheit weit über den Aktionsradius der IT hinausgeht. Informationssicherheit ist weit mehr als eine Teildisziplin der IT, und relevante Informationen müssen – angemessen aufbereitet – an das Management herangetragen werden.

Frage 6: Sind Ihnen Mehrwerte, die durch die Einführung eines Informationssicherheits-Management-Systems (ISMS) entstehen, bekannt oder dient das ISMS nur der Erfüllung regulativer Anforderungen? Durch strukturierte Koordination in einem ISMS nach ISO/IEC 27001:2013 bzw. durch IT-Grundschutz lassen sich Risiken gezielt identifizieren und behandeln und lässt sich Informationssicherheit ressourcenschonender, sicherer und zuverlässiger betreiben und so kontinuierlich auf allen Ebenen steigern. Daneben erfüllt das Unternehmen regulative Anforderungen (Compliance) und ist in der Lage, sein hohes Niveau in der Informationssicherheit gegenüber Dritten nachzuweisen, zum Beispiel durch eine Zertifizierung. Die Zertifizierung eines ISMS ist erfahrungsgemäß nicht nur förderlich für bestehende Kundenbindungen, sondern kann in Zeiten einer verstärkt sensibilisierten Öffentlichkeit das Neukundengeschäft positiv beeinflussen. **Arne Helemann** ■

www.tuv.com/informationssicherheit