Anforderungen durch das neue IT-Sicherheitsgesetz

Wie Firmen IT-Sicherheitsproblemen aktiv vorbeugen können

Holger Schellhaas, Ulrich Kolberg, Norbert Fuchs

Das "Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme", auch als IT-Sicherheitsgesetz bekannt, ist zum 25. Juli 2015 in Kraft getreten. Konkret schreibt dieses Gesetz Mindeststandards für die Informationssicherheit sowie eine Meldepflicht von Sicherheitsvorfällen für Betreiber sogenannter „kritischer Infrastrukturen" vor. Das sind Einrichtungen, „die für das Funktionieren des Gemeinwesens von zentraler Bedeutung sind", z.B. der Energie- und Gesundheitssektor, die Wasserversorgung, die Telekommunikation sowie das Finanz- und Versicherungswesen.

Diese Unternehmen werden verpflichtet, Cyberangriffe auf ihre Systeme unverzüglich dem BSI (Bundesamt für Sicherheit in der Informationstechnik) zu melden und ein vom BSI festgelegtes Mindestniveau an IT-Sicherheit einzuhalten. Alles in allem müssen etwa 2000 Unternehmen etwaige Cyberangriffe melden. Das BSI wertet die übermittelten Informationen aus, erstellt daraus ein Lagebild und warnt bei Bedarf andere Unternehmen. Bei Zuwiderhandlungen drohen bis zu 100.000 Euro Bußgeld.

Finanzdienstleistern ist das nicht neu, denn sie werden von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) verpflichtet, ein funktionierendes IT-Sicherheitsmanagement einzurichten, um die Sicherheit der IT-Prozesse und der IT-Systeme zu gewährleisten. Versicherungen in der EU müssen bereits seit 2013 **Solvency II** erfüllen und damit Mindestanforderungen an das Risikomanagement, insbesondere an operationale Risiken, umsetzen. Die MaRisk (Mindestanforderungen für das Risikomanagement) der BaFin zählt konkrete Schutzkategorien der IT-Sicherheit auf und verweist auf die gängigen Standards, nämlich die ISO 27001 und den **IT-Grundschutz** des BSI.

Was bedeutet das konkret für die Unternehmen?

Warum setzt sich ein Unternehmen mit Informationssicherheit auseinander und strebt sogar eine Zertifizierung an? Oft nicht aus eigenem Antrieb, sondern weil es von Geschäftspartnern oder Aufsichtsbehörden erwartet wird, bei Ausschreibungen verbindlich vorgeschrieben oder zur Bewertung von Kreditwürdigkeit und Versicherungsrisiken erforderlich ist.

Version 1.4/2017

Die überwiegende Anzahl der Firmen, die dem neuen IT-Sicherheitsgesetz unterliegen, überprüfen ihre IT-Systeme und bessern bei Bedarf nach. So handeln die Unternehmen proaktiv und vermeiden kritische Situationen nach bestem Wissen und Gewissen, indem sie die Risiken der IT angemessen managen. Auch der Gesetzgeber erachtet dieses Vorgehen als sinnvoll und empfiehlt konkret, sich an dem internationalen Standard ISO 27001 in der Fassung von 2013 zu orientieren. Die ISO-Norm erhebt den Anspruch, alle Belange der Informationssicherheit abzudecken und mit den vorgeschlagenen Maßnahmen den geforderten Mindeststandard zu erreichen.

Unsere Erfahrungen mit Kunden bestätigen, dass die intelligente Umsetzung gängiger Standards direkt zur Minimierung der Risiken in den Geschäftsprozessen führt. Gemeinsam mit dem TCI-Partner SSP Europe führen wir beispielsweise ein IT-Compliance Transformationsprojekt bei einem mittelständischen Versicherungsunternehmen durch, einer Tochter des italienischen Generali-Konzerns. Wir begleiten eine bekannte Sparkassengruppe dabei, die Compliance-Ziele nach MaRisk umzusetzen und gleichzeitig die IT-Qualitätsziele und IT-Anforderungen der Kunden zu erfüllen. Ziel hierbei ist, die Verantwortlichen bei der Zertifizierungsfähigkeit nach ISO 27001 auf Basis des BSI IT-Grundschutzes tatkräftig zu unterstützen. Beide Projekte wurden nicht nur vom Vorstand bzw. der Geschäftsführung aufgesetzt, sondern von diesen auch aktiv begleitet, was sich als wesentlicher Erfolgsfaktor herausstellte.

Die oftmals geäußerte Meinung, Compliance mit gesetzlichen Vorgaben oder ISO-Standards bringe keine Sicherheit, sondern bedeute lediglich, die von Verbänden, Banken oder dem Gesetzgeber aufgestellten Regeln zu erfüllen, bestätigen sich nicht. Im Gegenteil: Die sukzessive Verankerung nachvollziehbarer Regeln und eines Sicherheitsbewusstseins bei den Mitarbeitern ist gerade heute eine der wichtigsten Maßnahmen und der wirksamste Schutz gegen die vielfältigen Bedrohungen.
Das dient auch dem Image: Die NÜRNBERGER Lebensversicherung z.B. tut Gutes und spricht auch darüber, dass sie erneut das „Deutsche IT- Sicherheitszertifikat nach ISO 27001 auf der Basis von IT-Grundschutz“ vom BSI erhalten haben. Hiermit verfolgt die NÜRNBERGER zwei Ziele: Umfang und Niveau der Sicherheitsmaßnahmen sollen sich an den betrieblichen Erfordernissen orientieren. Und es werden relevante Gesetze, Regularien und Richtlinien eingehalten.

Unser Vorgehen bei der Umsetzung

Image, Geschäftserfolg und Unternehmensstabilität hängen in entscheidendem Maße von qualifizierten Management-Systemen und Management-Prozessen zur Informationssicherheit ab. Wie setzt man sich so konkret und so einfach wie möglich mit den Herausforderungen auseinander?

Zum einen geht es darum, die technischen Schwachstellen zu identifizieren - für Security-Tests binden wir hier Partner mit exzellenter Expertise ein, z.B. SEC4YOU Advanced IT-Audit Services aus Österreich. Zum anderen gilt es, das Bewusstsein für IT-Sicherheit zu verändern, den IT-Betrieb vom Management auf „Zuruf“ in geregelte Abläufe überzuführen und die IT-Infrastruktur auf ein angemessenes Sicherheitsniveau zu bringen – und das alles behutsam, schrittweise und mit Augenmaß, damit die Maßnahmen im Tagesablauf integriert und im Bewusstsein aller Beteiligten verankert werden.

Die Standards geben hier hervorragende Leitlinien vor: die ISO 27001 sagt, was zu tun ist, der BSI IT-Grundschutz sagt, wie es zu tun ist und wird damit deutlich konkreter. In beiden Fällen geht es um ein Managementsystem, welches wir Schritt für Schritt gemeinsam mit unseren Auftraggebern erarbeiten und umsetzen. Mit Hilfe von langjährig erprobten Bausteinen, deren Effektivität und Wirksamkeit sich bewährt haben:

1. **Aufbau des Managementsystems zur Informationssicherheit**
   Gemeinsam mit den Leitern der Organisation, des Risikomanagements und der IT wird der „Scope“ auf die kritischen Kernprozesse gelegt.
2. **Teilhabe des Managements**
   Die Bewertung der kritischen Geschäftsprozesse ist der Einstieg zur aktiven Einbeziehung der Unternehmensleitung. Anschließend erfolgt die Erstellung und Verabschiedung unternehmensweiter Richtlinien und Verfahrensanweisungen (Standard Operating Procedures, SOPs) zum Management der IT-Sicherheit.
3. **Bewertung wesentlicher Bausteine mit dem Health Check Informationssicherheit**
   Der Health Check Informationssicherheit ist eine schnelle und kostengünstige Alternative zu aufwändigen Analysen. Er ist ein geeignetes Instrument, um ein Reifegrad-Gutachten zu erstellen, die „Readiness“ für die geforderten Anpassungen an Standards zu messen und Maßnahmen abzuleiten.

4. **Maßnahmen zur Erreichung eines Mindeststandards**

   Das Ergebnis des Health Checks zeigt oft, dass die technische Umsetzung in der Praxis häufig gar nicht so schlecht ist, vielfach sogar besser als erwartet. Es fehlen jedoch Dokumente und Nachweise zur unternehmerischen Risikovorsorge, die Betriebshandbücher sind nicht einheitlich, Installationen laufen nicht standardisiert, Abläufe sind unverständlich. Die ISO- und BSI-Standards helfen beim Aufräumen: Passende Regeln werden eingeführt, die Dokumentation wird optimiert und alles Überflüssige, nicht Wertschöpfende abgebaut.

5. **Sensibilisierung von Managern und Mitarbeitern**

   Zur Sensibilisierung der Manager und Mitarbeiter in der IT und im Fachbereich entwickeln wir **Awareness-Programme,** Trainings und Kampagnen und führen diese auf Kundenwunsch auch selbst durch.

Zusammenfassung

Wir beraten seit vielen Jahren erfolgreich Finanzdienstleister, Telekommunikationsunternehmen und Energieversorger und kennt deren spezifische Anforderungen. Kein Unternehmen ist wie das andere, daher verlangt die Umsetzung der Anforderungen des IT-Sicherheitsgesetzes eine gesamtheitliche, strategische Betrachtung und Herangehensweise zum Thema IT-Compliance. Das neue IT-Sicherheitsgesetz zeigt, dass Transparenz einen nicht unerheblichen Beitrag zur Performance-Verbesserung leistet.

In konkreten Projekten zur Informationssicherheit haben wir nachgewiesen, dass nicht nur der Standard ISO 27001, sondern auch das aufwändigere Vorgehen nach BSI Grundschutz geeignete Mittel sind, um schrittweise ein angemessenes Sicherheitsniveau zu erreichen. Dies gilt auch für Kleinunternehmen. Der Organisationsaufwand wird hierbei so gering wie möglich gehalten und stört den Tagesablauf so wenig wie möglich.

Das ist Transformation im besten Sinne: Compliance rentiert sich!

Ein Angebot der convio Leadership Consulting
Steingarten 5A | 22175 Hamburg | Tel: +49 40 1801 2101 | Fax: +49 40 1801 2102 | info@ictsourcing.de