inge HANSCHKE

INFORMATIONS-SICHERHEIT UND DATENSCHUTZ

EINFACH & EFFEKTIV

Integriertes Management-instrumentarium systematisch aufbauen und verankern

HANSER

Zunehmende Cyber-Angriffe sowie gesetzliche und Compliance-Anforderungen, wie die EU-DSGVO, erfordern eine deutlich höhere Aufmerksamkeit in den Unternehmen für Informationssicherheits- und Datenschutzfragestellungen. Für die Festlegung eines integrierten Managementsystems für Informationssicherheit und Datenschutz müssen die Anforderungen verstanden und im Kontext des Unternehmens bewertet werden.

Die Anforderungen in der Informationssicherheit und im Datenschutz für Unternehmen sind vielfältig. Der Umgang mit Cyber-Security und die Erfüllung von gesetzlichen und Compliance-Anforderungen, wie die EU-DSGVO, sind hierfür Beispiele. Die immer weiter zunehmende Durchdringung von Informationstechnik in den Geschäftsprozessen, die steigende Bedrohungslage sowie gesetzliche und Compliance-Anforderungen führen zu Gefahren, wie

- Missbrauch oder Verlust von schützenswerten Daten,
- Verstöße gegen gesetzliche Bestimmungen oder unternehmensspezifische Richtlinien und Regeln mit zum Teil persönlicher Haftung und
- Behinderung oder sogar Unterbrechung der Geschäftstätigkeit durch z. B. nicht verfügbare Systeme.

Diese Bedrohungslage nimmt immer weiter zu. Gründe sind hierfür u. a.:

- Steigender Vernetzungsgrad: Menschen und IT-Systeme arbeiten zunehmend vernetzt (horizontal und vertikal siehe [Han18]) auch über Unternehmensgrenzen hinweg. Eine Sicherheitslücke kann nicht isoliert, sondern muss mit ihren Abhängigkeiten betrachtet werden.
- IT-Verbreitung und Durchdringung: Immer mehr Bereiche werden von der Informationstechnik durchdrungen. Beispiele sind Smart Home oder RFIDs zur Steuerung von Besucher- oder Warenströmen oder IT-gestützte Sensorik in Autos, um automatisch auf veränderte Umgebungsverhältnisse reagieren zu können. Die verschiedenen IT-Komponenten kommunizieren miteinander zunehmend drahtlos und sind über das Internet lokalisierbar und steuerbar.
- Zunehmende und schnellere Ausnutzung von Schwachstellen: Die Zeitspanne zwischen dem Bekanntwerden einer Sicherheitslücke und den ersten gezielten Massenangriffen (z. B. Computerviren, Trojanische Pferde oder andere Angriffe) sinkt immer weiter. So muss zunehmend schneller die Information über Sicherheitslücken und deren Beseitigung, z. B. durch Einspielen von Patches und Updates, bekannt sein. Ein gut aufgestelltes Informationssicherheitsmanagement mit Warnsystem ist extrem wichtig, um schnell die richtigen Maßnahmen zu ergreifen.

Neben den zunehmenden Bedrohungen der Cyber-Security sind die steigenden Anforderungen aus Datenschutz und Informationssicherheit aufgrund der EU-Datenschutz-Grundverordnung (siehe [Voi18]) und in der Informationssicherheit entsprechend der individuellen Anforderungen oder gesetzlichen Vorgaben zu bewältigen.

1.2.1 Wesentliche Normen und gesetzliche Vorschriften

ISO/IEC 2700X

ISO/IEC 2700X ist die De-facto-Normenreihe für die Informationssicherheit. Die Sicherheitsstandards der ISO/IEC-2700X-Normenreihe zielen darauf ab, das Sicherheitsniveau in Unternehmen zu verbessern. Die ISO/IEC 2700X enthält Anforderungen und Maßnahmen für den Aufbau, Betrieb und die kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems (ISMS). Die Anforderungen der Norm sind durch die Implementierung von für das Unternehmen passenden Sicherheitsmechanismen zu erfüllen. Siehe hierzu Abschnitt 1.2.3.

In Abschnitt 1.2.3 unter der Zwischenüberschrift „TISAX“ finden Sie Informationen über TISAX, einen Standard für externe Zulieferer und Dienstleister der Automobilindustrie. Dieser erweitert die ISO/IEC 27001 um branchenspezifische Anforderungen.

IT-Grundschutz (IT-GS)

Der IT-Grundschutz ist eine Methodik für einen praktikablen und aufwandsarmen sowie angemessenen Schutz von Informationen, um das Informationssicherheitsniveau in Unternehmen zu erhöhen. Er liefert einen De-facto-Standard für IT-Sicherheit. Er wird vom Bundesamt für Sicherheit in der Informationstechnik (kurz BSI) (weiter-)entwickelt und in regelmäßigen Abständen mit den internationalen Normen wie ISO/IEC 27001 abgeglichen. Siehe hierzu Abschnitt 1.2.4.

IT-Sicherheitsgesetz (ITSG)

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, um den Gefahren beim Ausfall von kritischen Infrastrukturen zu begegnen

Am 3. Mai 2016 ist der erste Teil der BSI-KRITIS-Verordnung (§ 10 BSI-Gesetz) in Kraft getreten. Hier werden neben dem BSI-Gesetz auch das **Energiewirtschaftsgesetz (EnWG)**, das Telemediengesetz, das Telekommunikationsgesetz und weitere Gesetze geändert und ergänzt.

Im Vordergrund stehen Betreiber sogenannter „kritischer Infrastrukturen“.

Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Diese müssen innerhalb von vorgegebenen Fristen (zwei Jahre) Mindeststandards für IT-Sicherheitsmaßnahmen in den kritischen Branchen wie Energie oder Gesundheit entwickeln und nachweislich umsetzen. Zudem besteht bei Ausfällen oder IT-Sicherheitsvorfällen Meldepflicht gegenüber dem BSI sowie Informationspflichten gegenüber betroffenen Nutzern.

EU-DSGVO

Die europäische Datenschutz-Grundverordnung (EU-DSGVO) zur Vereinheitlichung des Datenschutzrechts in Europa

Schwerpunkt der EU-DSGVO liegt auf der Stärkung der Rechte der Betroffenen (Auskunftsrecht und Recht auf Vergessen) sowie Rechenschaftspflicht der Verantwortlichen zum Nachweis der Grundsätze für die Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit, zeitliche Beschränkung, Integrität und Vertraulichkeit der Datenverarbeitung. Siehe hierzu Abschnitt 1.2.5.

DIN EN ISO 14001, Umweltmanagement für Umweltschutz

Die Bedeutung des Umweltmanagements wächst sowohl im öffentlichen Interesse als auch auf strategischer Ebene im Unternehmen zusehends. Eine Zertifizierung nach DIN EN ISO 14001 erfordert zwar ein Umweltmanagementsystem, hat aber das Potenzial für Ressourceneinsparungen und stärkt die Wettbewerbsfähigkeit des Unternehmens.

Jedoch gibt es natürlich gerade bei Verfahrens- und Arbeitsanweisungen Überlappungen zu einem ISMS. Diese sollten durch ein integriertes Managementsystem eliminiert werden.

ISO 20000 auf Basis der ITIL (siehe [Buc07])

Die Norm ISO/IEC 20000 wurde auf Basis der IT Infrastructure Library (ITIL) erarbeitet. Auf dieser Grundlage kann ein Service-Management-System zertifiziert werden. ITIL, vom britischen Office of Government Commerce (OGC) entwickelt, ist eine Ansammlung mehrerer Bücher zum Thema „IT-Service-Management“. Das allgemeine Ziel von ITIL ist die Verbesserung der Qualität von IT-Dienstleistungen, der Kosteneffizienz und ein funktionierender IT-Betrieb. Informationssicherheit wird aus der operativen Perspektive der verschiedenen Services, wie Service Support und Service Delivery, heraus betrachtet. Service Support stellt alle operativen Prozesse bereit, die zur Behandlung von Service-Unterbrechungen und zur Durchführung von Änderungen dienen. Somit wird die Aufrechterhaltung der IT-Services garantiert. Service Delivery stellt sicher, dass verbindliche Rahmenbedingungen für die operativen Prozesse bestehen. Es regelt die planerischen, vertraglichen und finanziellen Themen.

NIST (National Institute of Standards and Technology)

Die US-amerikanische Bundesbehörde NIST ist u. a. für die Entwicklung von Standards zuständig. Diese Standards sind für US-Behörden verpflichtend. Zudem veröffentlicht das NIST in der Reihe Special Publication 800 („NIST SP 800“-Serie) regelmäßig Dokumente zu Informationssicherheit-Themen, wie Kryptografie oder Cloud-Computing. Die Standards und die Dokumente haben international einen weitreichenden Einfluss auf die Gestaltung der Informationssicherheit. Insbesondere das Dokument „NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations“ stellt für den Bereich Sicherheitsmanagement eine große Zahl an Kontrollen für den Schutz von Informationsverbünden zusammen. Die Kontrollen sind nach zusammengehörigen Bereichen, wie z. B. Schulung und Sensibilisierung, Berechtigungsmanagement oder Infrastruktursicherheit, gegliedert.

PCI DSS (Payment Card Industry Data Security Standard) des PCI Security Standards Council

PCI DSS formuliert Sicherheitsanforderungen an die Abwicklung von Kreditkartentransaktionen, d. h. wenn eine Zahlungskartennummer, eine PAN (Primary Account Number), gespeichert, verarbeitet oder übermittelt wird. PCI DSS bezieht sich hierbei auf Karteninhaberdaten, die in Verbindung mit der PAN gespeichert werden. Dies sind laut PCI DSS der Name des Karteninhabers, der Servicecode und das Ablaufdatum der Karte.

Vertrauliche Authentisierungsdaten, wie z. B. die Daten des Magnetstreifens einer Debit- oder Kreditkarte, PINs und Kartenprüfwerte wie z. B. der CVC2 (Card Validation Code Version 2), haben einen sehr hohen Schutzbedarf. Diese dürfen nach der Authentisierung nicht in den Händlersystemen gespeichert werden.

Die Anforderungen von PCI DSS müssen von allen Unternehmen umgesetzt werden, die Karteninhaberdaten von Kreditkarten speichern, verarbeiten oder übertragen. Beispiele sind Händler, die Kreditkartenzahlungen akzeptieren, Hosting-Anbieter oder Dienstleister, die diese im Auftrag weiterverarbeiten, sowie alle Dienstanbieter, die auf Karteninhaberdaten zugreifen können.

Die erfolgreiche Umsetzung muss überprüft und das Ergebnis registriert werden. Je nach Art und Größe der Institution, der Anzahl der Transaktionen und der Führung der Karteninhaberdaten, gibt es hierzu verschiedene Möglichkeiten von Zertifizierungen oder Selbstzertifizierungen. Wenn eine Zertifizierung nicht zwingend notwendig ist, kann durch jährlich auszufüllende Selbstbeurteilungsfragebögen die Konformität zum PCI-Regelwerk mitgeteilt werden.

Anforderungen des PCI DSS sind hierbei insbesondere:

- Erstellung und Wartung eines sicheren Netzwerks mit Sicherheitszonen (Firewall) sowie regelmäßige Überwachung und regelmäßiges Testen von Netzwerken inklusive Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten
- Ändern der vom Anbieter festgelegten Standardeinstellung für Systemkennwörter und andere Sicherheitsparameter
- Schutz von Karteninhaberdaten sowie Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze
- Verwendung und regelmäßige Aktualisierung von Antivirussoftware
- Vorgabe und Einhaltung von Richtlinien für eine sichere Systementwicklung (siehe Abschnitt 2.2)
- Implementierung starker Zugriffsschutz- und Kontrollmaßnahmen mit u. a. Zuweisung einer eindeutigen ID für jede Person mit Zugriff sowie Beschränkung des physischen Zugriffs auf Karteninhaberdaten

KonTraG, das Gesetz zur Kontrolle und Transparenz im Unternehmen

Wesentlich sind hier insbesondere die Verpflichtung zur Einrichtung eines Kontrollsystems mit verbindlichen Regeln im Unternehmen und ein