Informationssicherheit als Prozess

Der Schutz des Geschäftswertes „Information“ vor Bedrohungen hat sich im Laufe der letzten Jahre unter dem Namen „Informationssicherheit“ einen Spitzenplatz unter den Voraussetzungen für moderne Geschäftsprozesse in der Wirtschaft und Verwaltung erobert.

Unternehmen und Behörden, die bestrebt sind, an sie gestellte gesetzliche, vertragliche und sonstige Anforderungen stets angemessen zu erfüllen und – gleichzeitig – geschäftsschädigende Vorfälle (durch Begrenzung von Risiken) nachhaltig zu vermeiden, kommen an einem Informationsschuz nicht vorbei.

Eine umfassende Informationssicherheit, basierend auf der dauerhaften Erfüllung der Anforderungen und nachhaltigen Begrenzung der Risiken, wirkt außerordentlich komplex und dynamisch. Sie macht zum einen Managementinstrumente zur Planung, Realisierung und Betrieb, Überwachung sowie kontinuierlichen Verbesserung unabdingbar. Zum anderen erfordert der Informationssicherheits-Prozess eine vernünftige Steuerung, die durch ein System von Verfahren, Prozeduren und Regeln zum Management der betrieblichen (behördlichen) Informationssicherheit übernommen werden soll. Ein solches System wird Informationssicherheits-Managementsystem (ISMS) genannt.

Sicherheitsstandards

Vor ungefähr zehn Jahren war noch viel Kreativität notwendig, damit eine Organisation die Informationssicherheit für sich als Prozess entdecken und mittels eines ISMS steuern konnte und die meisten Unternehmen und Behörden fühlten sich dabei überfordert. Heute genügt es, auf vorhandene, breit anerkannte und Praxis erprobte Standards zurückzugreifen.

Zu den Letzteren gehört insbesondere der internationale Standard ISO 27001 „Management von Informationssicherheit – Anforderungen“, begleitet von ISO 17799 „Leitfaden zum Management von Informationssicherheit“. Auf deren Basis wird derzeit bei der ISO die Standardreihe ISO 27000 ff. (ISO 27000-27009 …) entwickelt, die die Umsetzung der ISO 27001 insgesamt erleichtern sollte.

Andererseits bieten die Standards 100-1…3 des Bundesamtes für Sicherheit in der Informationstechnik samt der dazugehörigen IT-Grundschutz-Kataloge, wie auch die ISO 27001, einen umfangreichen Leitfaden zum Management jeder organisationsweiten IT-Sicherheit. Kleine Bemerkung am Rande: Das BSI benutzt den Begriff IT-Sicherheit als Synonym für Informationssicherheit und begründet dieses mit der Verbreitung und dem Bekanntheitsgrad des Begriffs „IT-Sicherheit“.

Der entscheidende Vorteil des BSI-Ansatzes im Vergleich zu ISO 27001 und ISO 17799 ist eine klar gegliederte Sammlung praxisnaher IT-Sicherheitsmaßnahmen sowie Darlegung von deren Wechselwirkungen. Somit bietet der IT-Grundschutz eine hervorragende Basis für die systematische Planung, Anwendung und Bewertung der IT-Sicherheit in Behörden, Unternehmen und öffentlichen Institutionen. Dies führt dazu, dass das der Grundschutz nach BSI in vielen solchen Institutionen die Basis für die tägliche Arbeit des IT-Sicherheitsmanagements sowie für die kontinuierliche Umsetzung von Standard-Sicherheitsmaßnahmen bildet.

Insgesamt sind die BSI-Regelwerke sowohl für die Informationstechnik von Unternehmen und Behörden als auch für die damit verbundene Geschäftsprozesse, Fachaufgaben und Organisationsstrukturen anwendbar. Das BSI sieht im IT-Grundschutzansatz der BSI-Standards 100 (einschl. der IT-Grundschutz-Kataloge) einen ISMS-Ansatz, der zu den Anforderungen der ISO 27001 vollständig kompatibel ist und eine strukturierte und praxisorientierte Vorgehensweise sowie konkrete, detailliert beschriebene Maßnahmen zur Umsetzung der ISO 27001 bietet. Das BSI selbst begründet diese Aussage insbesondere mit tiefgehenden Untersuchungen und Vergleichsstudien. Feststellbar ist auf jeden Fall, dass diese Sicht auch auf der praktischen Seite – das heißt in der Fachwelt, bei Anwendern und

Abbildungen: TÜViT, photocase.com

in der Öffentlichkeit – zunehmende Anerkennung findet.

Nach unserer Auffassung liefert insbesondere der vorbeugende Charakter des BSI-Ansatzes einen wichtigen Beitrag zur Erhöhung der Effektivität und insbesondere der Effizienz der IT-Sicherheit und empfiehlt sich somit als einen wesentlichen Grundbaustein für jedes Vorhaben zur Etablierung einer umfassenden, ganzheitlichen Informationssicherheit.

Geodaten mit BSI-Siegel

Um die Transparenz der IT-Sicherheit in Organisationen nach innen und außen zu ermöglichen, hat das BSI zu Beginn des Jahres 2006 die „Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz“ eingeführt. Auf dem Weg zum IT-Grundschutz-Zertifikat können interessierte Organisationen in Folge durchgeführter Prüfungen bis zu zwei so genannte Testate („Einstiegsstufe“ und „Aufbaustufe“) durch BSI-lizenzierte Auditoren erhalten. Diese Möglichkeit erleichtert den Einstieg in den Zertifizierungsprozess, erlaubt eine Strukturierung der notwendigen Aktivitäten und erlaubt es der Organisation, den Fortschritt des eigenen IT-Sicherheitsprozesses auf der Basis einer qualifizierten und unabhängigen Prüfung nach innen und außen zu kommunizieren.

Während für die Erlangung eines Auditor-Testates der Einstiegsstufe die Organisation nur die für sich zutreffenden „unabdingbaren“ Maßnahmen (Stufe A) erfüllen muss, ist im nächsten Schritt (zur Erreichung der Aufbaustufe) auch die Erfüllung der sogenannten „wesentlichen“ Maßnahmen (Stufe B) erforderlich. Um ein nach ISO 27001 auf der Basis von IT-Grundschutz zertifizierbares Niveau zu erreichen, sind – neben den bereits erwähnten – auch die sogenannten „wichtigen“ Maßnahmen (Stufe C) sowie zusätzliche oder verstärkte Maßnahmen, die sich aus Risikoanalysen ergeben, erforderlich.

Die Bedeutung des begehrten BSI-Siegels im Kontext des sicheren Umgangs mit Geoinformationen resultiert daraus, dass diese eine Basis für Planungen und Entscheidungen in der Verwaltung, Wissenschaft und Wirtschaft bilden. Ihre Bedeutung hat in den vergangenen Jahren stetig zugenommen. Schon heute werden in rund der Hälfte aller Wirtschaftszweige Geoinformationen direkt oder indirekt genutzt. Dabei trägt eine gut ausgebaute und unter den Aspekten Verfügbarkeit, Integrität und Vertraulichkeit gut abgesicherte Geodateninfrastruktur (GDI) als Standortfaktor zu einer erfolgreichen Volkswirtschaft bei.

Unter diesen Aspekten erscheint eine BSI-Zertifizierung für alle Unternehmen und Behörden sinnvoll, die Geoinformationen generieren, beschaffen, verarbeiten, nutzen und transferieren. Nicht der kommerzielle oder nicht-kommerzielle Hintergrund der Handlung ist hierfür maßgebend, sondern die Tatsache, dass allein der Umgang mit solchen Informationen ein bemerkenswertes Schadenpotenzial für die eigene Organisation, Geschäftspartner und Dritte verbirgt. Somit sind sowohl Verwaltungsbehörden, als auch Anbieter von Kartenmaterial, Marktforschungsinstitute, Adresshändler, Banken, Versicherungen, Versandhäuser und alle sonstigen Anbieter und Abnehmer, also Nutzer, von Geodaten gefordert.

Als Sicherheitsziele im Umgang mit Geoinformationen gelten beispielsweise:

- die Wahrung der Vertraulichkeit (gegenüber Fremden und auch gegenüber den eigenen Mitarbeitern), sowohl zum Schutz der Privatsphäre, als auch zum Schutz vor unbefugter wirtschaftlicher Verwertung
- die Wahrung der Integrität (Manipulationssicherheit), relevant insbesondere für kritische Bereiche (wie etwa nationales Interesse, Safety, Privacy.)
- die Wahrung der Verfügbarkeit, zum Beispiel bei Einbindung in Workflows (Business Continuity Aspekte)

Praxisorientierter Rahmen

Selbst wenn die Qualifizierung nach IT-Grundschutz stufenweise erfolgt, bleibt der Prozess zur Erreichung eines ISO 27001-Zertifikates auf der Basis von IT-Grundschutz oft aufwändig und zeitintensiv. Oft sind die vielfältigen Sicherheitsprobleme und -lücken einer Organisation im Vorfeld nicht bekannt und werden erst im Laufe der Vorbereitung auf die Zertifizierung entdeckt. Dies führt dazu, dass die Erstellung und kontinuierliche Anpassung der Dokumentation zum IT-Sicherheitsprozess in mehreren Iterationen erfolgt und einen erheblichen Aufwand erfordert.

Um der obern erwähnten kausalen Kette entgegenzuwirken und den Aufbau von IT-Sicherheitsprozessen nach BSI zu beschleunigen, hat TÜViT in seiner Rolle als Informatik TÜV einen praxisorientierten Rahmen für BSI-Zertifizierungsprojekte, begleitet von einem zielgerichteten Unterstützungsmodell unter dem Namen AKTÜV definiert.

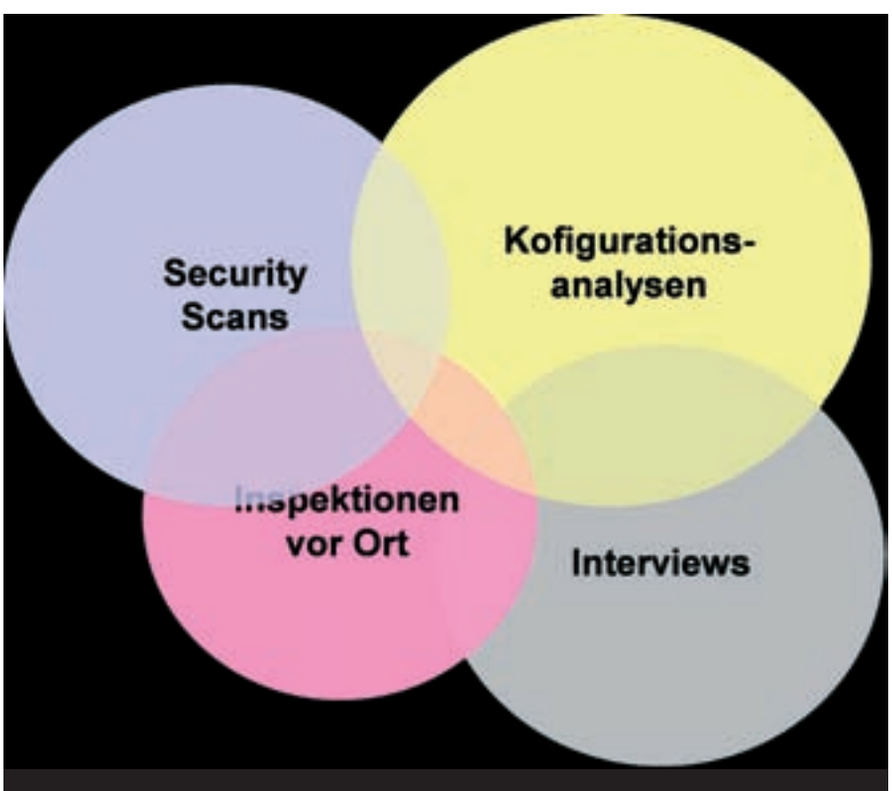
AKTÜV ist ein Phasenmodell der TÜV Informationstechnik GmbH, basierend auf:

- Analyse des IT-Sicherheitszustandes
- Konzeption des IT-Sicherheitsprozesses
- Testat oder Zertifizierung
- Überwachung
- Verbesserung

Analyse des IT-Sicherheitszustandes

Zu diesem Zweck empfiehlt TÜViT die Durchführung eines auf zentrale Vor- ▶

Techniken des IT-Grundschutz-Assesments.

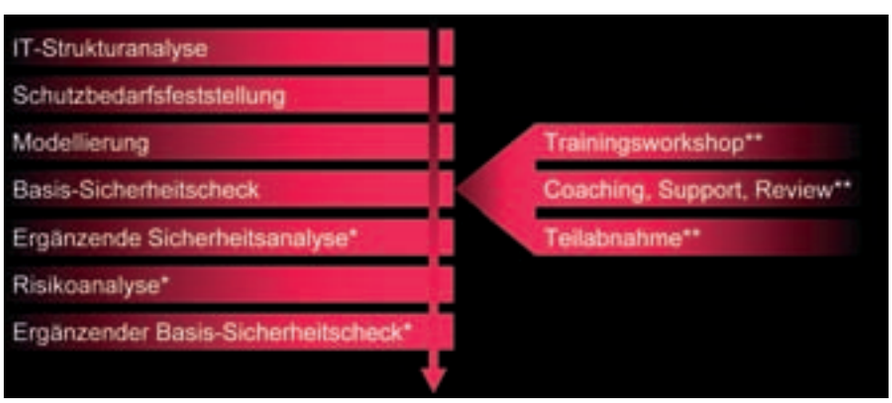


gaben der BSI-Standards fokussierten Assessments bereits im Vorfeld der Anwendung der IT-Grundschutzmethode. Ein solches Assessment ermöglicht zeitnah, für einen definierten IT-Verbund den aktuellen Status in Bezug auf IT-Grundschutz zu ermitteln, auf Problemfelder, Sicherheitslücken und Möglichkeiten zur Behebung hinzuweisen und so den Weg bis hin zu einer BSI-Zertifizierung abzukürzen. Nach Behebung der festgestellten Probleme wird die Anzahl der noch bestehenden Probleme und auch der notwendigen Iterationen, was den Gesamtaufwand beeinflusst, bis zur Erreichung und BSI-konformen Dokumentierung des IT-Grundschutzes erheblich geringer sein.

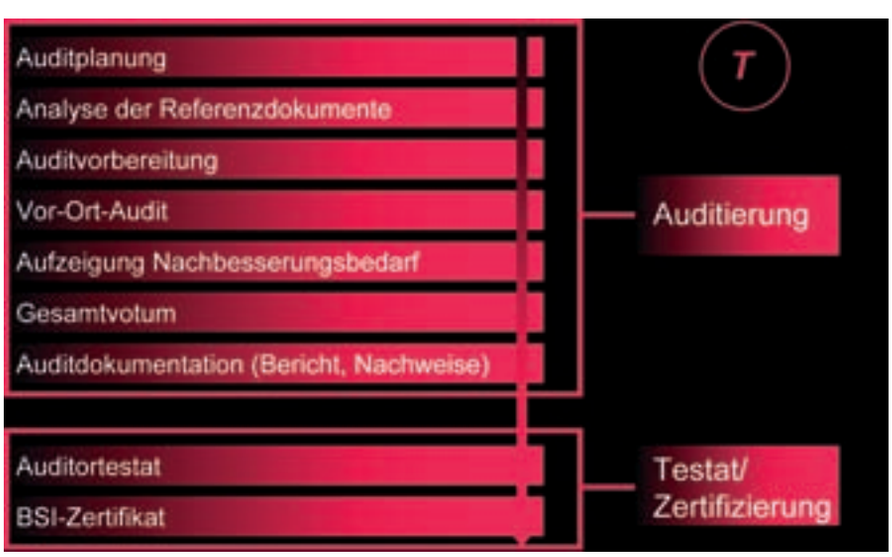
Wurde in einer Behörde oder in einem Unternehmen der IT-Grundschutz bisher nicht betrachtet, kann aber das Ergebnis eines solchen Assessments auch sein, dass bereits eine Vielzahl der geforderten IT-Grundschutzmaßnahmen umgesetzt sind. Hiermit eröffnet sich für die Institution die Möglichkeit einer relativ kurzfristigen Testierung oder sogar die Perspektive einer baldigen Zertifizierung.

Praktische, langjährige Erfahrungen der TÜV Informationstechnik GmbH mit dem Aufbau einer Methodik zum IT-Grundschutz-Assessment zeigen, dass insbesondere die Kombination von technischen Netzwerk- und Systemprüfungen mit Inspektionen, Konfigurationsanalysen und schließlich auch Interviews zu einer komplexen, effektiven und effizienten Betrachtung der IT-Sicherheit in der Institution führen. Das von TÜViT definierte, bottom-up orientierte Assessment-Verfahren konzentriert auf der einen Seite die Vielzahl der praktischen IT-Sicherheitsaspekte in der Organisation auf wesentliche Kernpunkte (Sicherheitsmanagement, Organisation, Personal, Infrastruktur, Technik) die von den Verantwortungsträgern verstanden und synergetisch gesteuert werden können. Auf der anderen Seite ermöglicht ein ausführlicher Assessmentbericht die Identifizierung und Behandlung der der gefundenen Schwachstellen im Detail. Zur Erleichterung des Controllings der Problembehebung sind die detailliert dokumentierten Schwachstellen auf Schwachstellengruppen, Kernaspekte und Schichten der IT-Sicherheit gemappt.

Durch die strukturierte, auf wesentliche Sicherheitsaspekte fokussierte Vorgehensweise kann ein IT-Grundschutz-Assessment die Effektivität und Effizienz des Grundschutzvorhabens einer Organisation erheblich steigern und Zertifizierungsprozesse beschleunigen.



TÜViT-Modell der methodischen Unterstützung.



Testat und Zertifizierung des IT-Sicherheitsprozesses.

IT-Sicherheitsprozess

In dieser Phase werden die Sicherheitsprobleme und -schwachstellen anhand des Assessmentberichtes angegangen, priorisiert und schließlich auch behoben. Danach steht der Etablierung eines IT-Sicherheitsprozesses nach BSI-Standard 100-2 (Übernahme der Verantwortung für die Sicherheit durch das Management, Verabschiedung einer IT-Sicherheitsleitlinie, Definition einer IT-Sicherheitsorganisation, Ressourcenzuweisung für die IT-Sicherheit) nichts mehr im Wege.

Parallel dazu ist auch die IT-Sicherheitskonzeption nach BSI-Standard 100-2 anzugehen und die sogenannten „defizitären“ Maßnahmen zu implementieren.

Auch in dieser Phase erweisen sich einige Unterstützungsleistungen durch externe Partner als sinnvoll, zum Beispiel die Durchführung von Tests und Reviews nach Behebung der im Assessment identifizierten Sicherheitsprobleme und -schwachstellen und später auch nach Realisierung der noch „defizitären“ Maßnahmen. Das TÜViT-Modell der methodischen Unterstützung (Training, Coaching, Support) zur Etablierung des IT-Sicherheitsprozesses und zur IT-Sicherheitskonzeption garantiert den Aufbau und Verbleib des Know-hows innerhalb der Organisation.

Testat oder Zertifizierung

Hat der IT-Sicherheitsprozess die Testierungs- oder sogar die Zertifizierungsreife erreicht, sollte die Bestätigung durch einen qualifizierten, unabhängigen Dritten angestrebt werden. Berechtigt zur Durchführung der dazu notwendigen Third Party Audits nach dem Prüf- und Zertifizierungsschema des BSI sind grundsätzlich alle BSI-lizenzierten ISO 27001-Audi-

Abbildungen: TÜViT

toren auf der Basis von IT-Grundschutz, die von der zu auditierenden Organisation unabhängig sind.

Die Erteilung eines Testates erfolgt durch den Auditor selbst auf Basis der Auditergebnisse, die er in einem ausführlichen Auditbericht nach Vorgaben des beschriebenen Prüfschemas dokumentieren muss. Zur Erteilung eines Zertifikats erfolgt die die Prüfung der Auditergebnisse und die Zertifizierungsfreigabe durch das BSI. Die erteilten Testate und Zertifikate sind (außer bei gravierenden Veränderungen im Geltungsbereich) jeweils zwei Jahre gültig und werden auf der Website des BSI gelistet. Um auch weiterhin gelistet zu bleiben, ist vor/zum Ablauf der Gültigkeit die Erreichung einer höheren Qualifizierungsstufe oder die Rezertifizierung erforderlich.

Überwachung und Verbesserung

Ziel dieser Phase ist die Weiterentwicklung des IT-Sicherheitsprozesses und der dazugehörigen Unternehmensstrukturen und -abläufe in Richtung Business Excellence.

Wie bereits angedeutet, ist die Schaffung von IT-Sicherheit kein zeitlich begrenztes Projekt, sondern ein kontinuierlicher Prozess. Die Angemessenheit und Wirksamkeit aller Elemente des Managementsystems für Informationssicherheit muss ständig überwacht, überprüft und kontinuierlich verbessert werden. Dazu müssen Erkenntnisse über Schwachstellen und Verbesserungsmöglichkeiten genutzt werden und – wenn notwendig – auch zu Konsequenzen in der Sicherheitsorganisation führen. Wichtig ist es auch, zukünftige Entwicklungen sowohl bei der eingesetzten Technik als auch in Geschäftsprozessen und Organisationsstrukturen frühzeitig zu erkennen, um rechtzeitig potenzielle Gefährdungen identifizieren, Vorkehrungen treffen und Sicherheitsmaßnahmen umsetzen zu können.

Eine elementar wichtige Aktivität ist die regelmäßige Durchführung von Managementbewertungen, durch die die Angemessenheit und Wirksamkeit des IT-Sicherheitsprozesses und des ISMS von der obersten Leitungsebene überprüft und bewertet werden muss. Die Ergebnisse der Managementbewertung tragen – zum Beispiel durch Zuweisung weiterer Ressourcen – entscheidend zur ISMS-Verbesserung bei. Auch zu dieser Phase erweisen sich einige Unterstützungsleistungen durch externe Partner als sinnvoll, zum Beispiel die Durchführung von Tests und Reviews nach Behebung der Abweichungen und Empfehlungen aus dem Audit und später auch nach Realisierung weiterer Maßnahmen. Empfehlenswert ist auch die methodische Unterstützung zur Optimierung des IT-Sicherheitsprozesses und Weiterentwicklung der IT-Sicherheitskonzeption durch einen qualifizierten, externen Partner, in Form von Training, Coaching und Support.

Fazit

Der Deutsche Bundestag forderte in seiner Entschließung „Nutzung von Geoinformation in der Bundesrepublik Deutschland“ vom 15. Februar 2001 die Bundesregierung auf, den Aufbau einer nationalen Geodateninfrastruktur zügig voranzutreiben. Bund und Länder waren aufgerufen, in enger Zusammenarbeit die Chancen zu nutzen, die in den Geowissenschaften und Geoinformationen liegen.

Seitdem führen Behörden, Wirtschaftsunternehmen und Normungsgremien vielfältige Aktionen durch, um beispielsweise die Koordinierung auf dem Gebiet des Geoinformationswesens zu verbessern, Geodateninfrastrukturen konzeptionell weiterzuentwickeln sowie die technische und inhaltliche Vereinheitlichung des Handlings mit Geodaten zu realisieren.

Damit sowohl Nutzer, als auch Anbieter aus den öffentlichen Verwaltungen, Wirtschaft, Wissenschaft und Bürger die vorhandenen Geodaten künftig effektiver und effizienter in ihre Entscheidungsprozesse einbeziehen und dabei jeglichen Missbrauch wirksam verhindern können, ergibt sich eine dringende Empfehlung in Richtung sicherer Geodaten und Geoinfrastrukturen mit BSI-Siegel. Wie wir meinen – ein durchaus lohnenswertes und auch gut erreichbares Ziel. ■

DIPL.-ING. ADRIAN ALTRHEIN
Leiter Enterprise Security & ISMS
TÜV Informationstechnik GmbH
Leimbachstr. 227
57074 Siegen
Tel: +49 271 3378-195
Fax: +49 271 3378-197
Mobil: +49 160 888 5195
E-Mail: a.altrhein@tuvit.de
www.tuvit.de