PROZESSMETRIKEN FÜR DIE INFORMATIONSSICHERHEIT BETRIEBLICHER ANWENDUNGSSYSTEME

Carsten Dorrhauer
Haio Röckle
Institut für Wirtschaftsinformatik an der Hochschule Ludwigshafen
Ernst-Boehe-Str. 4, 67059 Ludwigshafen, Deutschland
E-mail: carsten.dorrhauer@hs-lu.de, haio.roeckle@hs-lu.de

EINLEITUNG

In vielen Unternehmen ist in den letzten Jahren die Informationssicherheit in den Fokus der Aufmerksamkeit gerückt, ihre Qualität wird aber kaum gemessen. Sicherheits-KPI wurden zwar vorgeschlagen (Jaquith 2007), haben sich aber in der Praxis bislang kaum durchgesetzt. (Schimpf und Röckle 2009). Im Gegensatz dazu werden die Prozesse des IT Service Management (ITSM) kontinuierlich evaluiert. In der Praxis haben Prozessframeworks, von denen ITIL das wichtigste ist, weite Verbreitung erfahren. ITIL sieht KPI zur Messung der Servicequalität für ITSM-Prozesse wie zum Beispiel Continuity Management und Incident Management vor. Allgemeiner betrachtet sind Prozess-KPI heutzutage weit verbreitet und akzeptiert, während Zustandskennzahlen – zumindest im Bereich der Informationssicherheit – offensichtlich schwieriger zu fassen sind.

Eine Ursache für die bemerkenswerte Vernachlässigung der Qualitätsmessung ausgerechnet bei Sicherheitsaspekten mag deshalb darin zu finden sein, dass die Vorgaben zur Informationssicherheit in den wichtigsten Standards nicht durchgängig prozessorientiert formuliert sind. So sind zwar die wesentlichen Vorgaben des Informationssicherheitsmanagements aus ISO 27001 prozessorientiert, nicht aber die Detailvorgaben nach ISO 27002. ITIL dagegen ist durchgängig prozessorientiert aufgebaut. KPI zur Messung der Qualität von ITIL-Prozessen sind bekannt und in vielen Fällen einfach zu implementieren und mit vertretbarem Aufwand zu erfassen.

Da aber die meisten Aufgaben der Informationssicherheit durchaus prozessorientiert durchgeführt werden, schlägt die vorliegende Arbeit eine prozessorientierte Sicht der Sicherheitsaufgaben vor, auf deren Grundlage prozessbasierte KPIs für die Informationssicherheit implementiert werden können. Dabei gibt es Kennzahlen, die

- den Prozess als solchen betreffen, z.B. „Welcher Anteil von sicherheitsrelevanten Zwischenfällen wird ohne Beteiligung des Servicedesk behoben?“ und solche, die
- seinen Output betreffen, z.B. „Welcher Anteil von sicherheitsrelevanten Zwischenfällen wird innerhalb einer vereinbarten Wiederherstellungszeit behoben?“

Die Unterscheidung zwischen diesen Kategorien ist fließend. Dem gegenüber stehen

- nicht-prozessbasierte Kennzahlen, die eindeutig rein technischer Natur sind, z.B. „Häufigkeit registrierter Portscans auf Webservern“.

Diese Arbeit konzentriert sich dabei auf Sicherheitsaufgaben im Zusammenhang mit betrieblichen Anwendungssystemen. Dadurch werden die Systeme erfasst, in denen die betrieblich relevanten Daten mit dem höchsten Schadenspotenzial verarbeitet werden, ohne sich in infrastrukturellen Details zu verlieren. Die Untersuchung erfolgt gegliedert nach den Lebenszyklusphasen betrieblicher Anwendungssysteme durch Betrachtung der jeweils relevanten Sicherheitsprozesse und der Anwendbarkeit prozessorientierter Sicherheitsmetriken. Bei der vorliegenden Arbeit handelt es sich um eine Neuauflage von Röckle und Dorrhauer 2011 mit einer knappen Reflektion über die Entwicklungen in den letzten Jahren.

INFORMATIONSSICHERHEIT UND IHRE MESSBARKEIT

Zu einem Managementsystem in einem Unternehmen gehören die Vorgabe von Zielen und ein Berichtswesen entlang der Unternehmensorganisation, das die Kontrolle der Ergebnisse ermöglicht. Nicht umsonst steht in Stellenbeschreibungen des Managements üblicherweise ein Passus wie „… berichtet an den CIO …“ oder „… berichtet direkt an den Vorstand …“.

Offensichtlich gibt es innerhalb eines Unternehmens mehrere Ebenen von Berichtsempfängern. Im Management der Informationssicherheit sind dies in der Regel der Informationssicherheitsmanager, häufig ISO oder CISO genannt, der IT-Leiter (CIO) und der IT-Vorstand, d.h. das Vorstandsmitglied in dessen Verantwortungsbereich die IT fällt. Jeder Berichtsempfänger hat unterschiedliche Informationsbedürfnisse:

- Der CISO interessiert sich für die einzelnen Sicherheitslücken, weil es zu seinen Aufgaben gehört, diese zu bewerten und ggfs. zu beheben.
- Der IT-Vorstand ist nur an Risiken interessiert, die für das Gesamtunternehmen relevant werden könnten oder die den Wertbeitrag der IT für das Unternehmen negativ beeinflussen könnten
- Der CIO interessiert sich für den qualitativen Gesamtzustand „seiner“ IT

Berichte können in unterschiedlichsten Formen und Formaten angefertigt werden. Grundsätzlich ist es wünschenswert, quantitative Kennzahlen zu haben, die aus Messungen gewonnen werden und die detaillierte Aussagen über Risikozustände, Fertigstellungsgrade, Qualitätszustände, etc. treffen. Der Managementvordenker Peter F. Drucker sagte z.B. nicht nur „If you can't measure it, you can't manage it", sondern auch "What gets measured gets managed" (Drucker 1974). Im Alltag sind solche quantitativen Kennzahlen leider häufig nicht vorhanden, so dass im Berichtswesen auf qualitative Informationen und subjektive Aussagen zurückgegriffen werden muss, dies ist aber nicht Thema dieser Arbeit.

Für das Management der Informationssicherheit wird vom wichtigsten Standard ISO 27001 ein „Maß für die Wirksamkeit der ausgewählten Maßnahmen…" gefordert (DIN2008a, Kap. 4.2.2, d), allerdings nicht weiter spezifiziert. Entsprechend findet sich im vertiefenden Standard ISO 27002 die Aussage „Das Messen von Informationssicherheit ist außerhalb des Geltungsbereichs dieses Standards" (DIN 2008a, Fußnote zu 0.7, j). Diese Lücke sollte geschlossen werden mit einem Standard ISO 27004, der nach einigen Jahren Entwicklungs- und Abstimmungsdauer im Dezember 2009 veröffentlicht wurde (ISO/IEC 2009), dessen praktische Verifikation aber noch aussteht (ISO/IEC 2011).

Bereits früher wurden zahlreiche IT Security Kennzahlen (Security Metrics) vorgeschlagen (Jaquith 2007). Die Menge an Kennzahlen ist allerdings gerade für Vorstände viel zu groß und die Relevanz der einzelnen Kennzahlen zu gering. Manche Kennzahlen sind auch aufgrund technischer Feinheiten für das höhere Management schlicht unverständlich. Dies sind Probleme, die auch mit dem Standard ISO 27004 weiterbestehen. Klassische Lösungsansätze bestehen darin, die Kennzahlen zu verdichten (aggregieren) und zu visualisieren, z.B. in Ampeldarstellungen oder in Dashboards („Management-Cockpit") bis hin zum Konzept einer „Balanced Security Scorecard". Weitere Ansätze des Security Reporting wurden in Schimpf und Röckle, Kap. 3 beschrieben.

Prinzipiell ist die Aggregation von Kennzahlen eine Aufgabe, die in jedem Unternehmensbereich in Angriff genommen werden muss. In Bezug auf das Management der Informationssicherheit gibt es aber zwei Besonderheiten:

- Gemäß den internationalen Standards zum Informationssicherheitsmanagement (BSI 2008, Funk 2011) soll der CISO direkt an den IT-Vorstand berichten, damit wird von der Aggregationslinie IT-Vostand – CIO – CISO abgewichen und es verstärkt sich die Gefahr, dass der IT-Vorstand mit einer Überzahl von Detailinformationen konfrontiert wird.
- Auch kleine Sicherheitslücken können große Auswirkungen haben. Jedes Detail, das bei der Aggregation der Informationen wegfällt, kann Basis eines fatalen Unfalls oder Angriffs werden und wäre damit – nachträglich betrachtet – durchaus Management-relevant gewesen.

Im folgenden Kapitel greifen wir die Idee aus Schimpf und Röckle, Kap. 3.6 auf und spezifizieren prozessorientierte Kennzahlen zur Informationssicherheit. Wir nutzen damit die folgenden Vorteile aus:

- Bei der Definition von Prozesskennzahlen handelt es sich um ein etabliertes Vorgehen,
- das speziell auch dem Management ad hoc verständlich ist.
- Viele Haftungsfragen bei IT-Unfällen können ausgeschlossen werden, wenn angemessen funktionierende Prozesse nachgewiesen werden.
- Durch die hierarchische Gliederung von Prozessen ergibt sich eine weitere Hierarchie, anhand der die Prozesskennzahlen aggregiert werden können.

Bei den folgenden Untersuchungen beschränken wir uns auf die Prozesse, die für den Lebenszyklus betrieblicher Anwendungssysteme relevant sind, einerseits weil dies dem Fokus der Jahrestagung entspricht, andererseits weil dadurch u.a. die Business-kritischen Anwendungen erfasst sind, die z.B. auch im Rahmen von Sarbanes-Oxley betrachtet werden müssen.

SICHERHEITSASPEKTE IN DEN LEBENSZYKLUSPHASEN BETRIEBLICHER ANWENDUNGSSYSTEME

Sicherheitsanforderungen für Betriebliche Anwendungssysteme nach ISO 27002

Die Stärke des Informationssicherheitsstandards ISO 27002 liegt darin, dass er die wesentlichen Bereiche der Informationssicherheit, speziell die wesentlichen Sicherheitsmaßnahmen für Unternehmen und andere Organisationen vollständig abdeckt, wobei absichtlich viele Freiheitsgrade bleiben. Zur Erfassung der speziellen Sicherheitsaspekte im Lebenszyklus betrieblicher Anwendungssysteme ist hier speziell das Kapitel (die „Domäne") 12: „Beschaffung, Entwicklung und Wartung von Informationssystemen" vorgesehen.

Allerdings berühren auch viele weitere Maßnahmenbereiche und Maßnahmen die Sicherheit der betrieblichen Anwendungssysteme, z.B. die Domäne „10 Betriebs- und Kommunikationsmanagement". Die folgende Tabelle gibt deshalb zunächst eine Übersicht über die Punkte des ISO 27002 Standards, die nach Ansicht der Autoren relevant für betriebliche Anwendungssysteme sind oder sein können. Da viele Punkte dieses Standards recht offen formuliert sind, könnten andere Betrachtungen aufgrund der Interpretationsspielräume auch zu anderen Ergebnissen kommen, dennoch sind wir der Ansicht, dass diese Aufstellung als Übersicht gut geeignet ist. Zur Übersichtlichkeit werden die Punkte häufig gekürzt dargestellt, für die vollständige Formulierung sei der Leser

auf den Originaltext des Standards verwiesen, ebenso wie auf die Inhalte der einzelnen Punkte.

Tabelle 1: Relevante Controls des ISO 27001 Standards

Punkt im ISO 27001	**Bezug zu betrieblichen Anwendungssystemen**
6.2.1 Sicherheitsanforderungen in Bezug auf externe Mitarbeiter	Anforderungen aus Sicht des Unternehmens, soweit externe Mitarbeiter in Entwicklung oder Betrieb mitarbeiten
6.2.2 Sicherheitsanforderungen bei Datenzugriff von Kunden	Anforderungen aus Sicht des Unternehmens, soweit Funktionen des Anwendungssystems von Kunden genutzt werden
6.2.3 Vereinbarungen mit Dritten	Verträge zur Unterstützung der o.g. Anforderungen
7 Klassifizierung von Informationen	Im Softwareentwicklungsprozess sollte der Sicherheitsbedarf des Programmcodes und der zu verarbeitenden Daten klassifiziert werden.
8.2.3 Zurücknahme von Zugangsrechten	Eigentlich bezieht sich Kapitel 8 des Standards auf „Personalsicherheit“ in Bezug auf Angestellte des Unternehmens. Speziell der Punkt 8.2.3 sollte aber auch auf externe Mitarbeiter angewandt werden.
9.1.2 Zutrittskontrolle 9.1.3 Sicherung von Büros, Räumen und Einrichtungen 9.1.5 Arbeit in Sicherheitszonen	Kapitel 9 des Standards bezieht sich auf physische Sicherheit. Bei geheimen Entwicklungen könnte es sinnvoll sein, die genannten Punkte auf Mitarbeiter in der Softwareentwicklung anzuwenden.
10.1.2 Änderungsverwaltung	Dieser Punkt des Standards wird vom ITIL Prozess Change Management abgedeckt.
10.1.3 Trennung von Verantwortlichkeiten	Dieser Punkt ist in Bezug auf betriebliche Anwendungssysteme noch komplexer als im ISO 27002, da er sich einerseits auf die Softwareentwicklung (vgl. „Analyse und Design“) und andererseits auf den ITIL Prozess beziehen kann.
10.1.4 Trennung von Entwicklung, Test und Produktion	Ist sowohl für die Code-Sicherheit als auch für die Sicherheit von Produktivdaten relevant.
10.2 Dienstleistungserbringung von Dritten 10.2.1 Vorgaben überwachen 10.2.2 Leistungen überprüfen 10.2.3 Change Mgmt. für Dienstleistungen von Dritten	Bezieht sich auf die Qualität der Leistungserbringung von externen Mitarbeitern im Gegensatz zu 6.2, wo es um „echte“ Sicherheitsanforderungen geht.
10.3.1 Kapazitätsplanung 10.3.2 Systemabnahme	Findet sich in den ITIL Prozessen *Capacity Management* und *Change Management*
10.4.1 Maßnahmen gegen Schadsoftware	Bezieht sich eigentlich auf Virenschutzmaßnahmen und wäre damit nicht relevant für betriebliche Anwendungssysteme. Kann aber auch darauf bezogen werden, dass der Code selbst entwickelter Software frei sein muss von Schadcode und fällt damit in den Bereich der Code Security
10.5.1 Backup von Informationen	Kann in Bezug auf betriebliche Anwendungssysteme so interpretiert werden, dass diese einen angemessenen Backup ermöglichen bzw. unterstützen. Dies kann in Bezug auf Softwareentwicklung aber auch in Bezug auf Auswahl und Implementierung von Software gesehen werden.
10.7.3 Umgang mit Informationen 10.7.4 Sicherheit der Systemdokumentation	In Bezug auf Softwareentwicklung ist zu beachten, dass der entwickelte Code und die Dokumentation einen angemessenen Umgang erlauben. Im Betrieb ist auf den Umgang mit Programmcode und -dokumentation zu achten.
10.8 Austausch von Informationen 10.8.1 Leitlinien und Verfahren 10.8.2 Vereinbarungen 10.8.3 Transport physischer Medien 10.8.4 Elektronische Mitteilungen 10.8.5 Geschäftsinformationssysteme	Ist in Bezug auf Softwareentwicklung in dem Sinne relevant, dass die entwickelte Software angemessene Sicherheit in den genannten Punkten erlaubt. Ist im Betrieb dahingehend relevant, dass die vorhandenen Möglichkeiten auch angemessen genutzt werden.

10.9 E-Commerce 10.9.1 E-Commerce 10.9.2 Online-Transaktionen 10.9.3 Öffentlich verfügbare Informationen	Analog zu den Anmerkungen zu 10.8
10.10 Überwachung (Audit) 10.10.1 Auditprotokolle 10.10.2 Überwachung der Systemnutzung 10.10.3 Schutz von Protokollinformationen 10.10.4 Admin. und Betreiberprotokolle 10.10.5 Fehlerprotokolle 10.10.6 Zeitsynchronisation	Analog zu den Anmerkungen zu 10.8
11 Zugangskontrolle 11.1 Geschäftsanforderungen 11.1.1 Leitlinie 11.6.1 Einschränkung von Informationszugriffen	Die Leitlinie muss sowohl bei der Entwicklung als auch im Betrieb von Anwendungen berücksichtigt werden. Es gelten die Anmerkungen zu 10.8
11.2 Benutzerverwaltung 11.2.1 Registrierung 11.2.2 Sonderrechte 11.2.3 Passwörter 11.2.4 Überprüfung 11.3.1 Passwortverwendung	Analog zu den Anmerkungen zu 10.8
11.5.4 Verwendung von Systemwerkzeugen	Im Betrieb soll der Zugriff auf administrative Funktionen der Software besonders geschützt werden, z.B. auf Betriebssystemebene. Bei der Softwareentwicklung muss darauf geachtet werden, dass die Anforderung im Betrieb erfüllt werden kann.
11.6.2 Isolation sensitiver Systeme	Ist eine Betriebsaufgabe für besonders sicherheitsrelevante Anwendungen

11.7.1 Mobile Computing und Kommunikation 11.7.2 Telearbeit	Generell gelten die Anmerkungen zu 10.8. Für Anwendungen auf mobilen Geräten sind ggfs. spezielle Schutzmaßnahmen zu treffen. Für Anwendungen, die per Telearbeit genutzt werden sollen, ist die entsprechende Kommunikationssicherheit zu gewährleisten. Beides gilt für die Entwicklung und für den Betrieb, vgl. die Punkte 10.8 und 10.9 des Standards.
12 Beschaffung, Entwicklung und Wartung von Informationssystemen 12.1.1 Analyse und Spezifikation von Sicherheitsanforderungen	Generell gilt das Prinzip, dass Informationssicherheit in jedem Projekt bereits in Analyse und Design berücksichtigt werden muss.
12.2.1 Überprüfung von Eingabedaten 12.2.2 Kontrolle der internen Verarbeitung 12.2.3 Integrität von Nachrichten 12.2.4 Überprüfung von Ausgabedaten	Generell handelt es sich hier um typische Elemente der Code Sicherheit, die in der Softwareentwicklung zu berücksichtigen sind. Allerdings ist es auch denkbar, weitere Prüfungen im Betrieb vor- und nachzuschalten, um die Sicherheit zu steigern. Insbesondere die Integrität von Nachrichten könnte durch Mechanismen der Netzwerkverschlüsselung und –signatur unterstützt werden.
12.3.1 Leitlinie Kryptografie 12.3.2 Schlüsselverwaltung	Der Bedarf an Kryptografie muss in den einzelnen Projekten ermittelt werden. Falls Kryptografie genutzt wird, müssen die Schlüssel angemessen geschützt werden. Außerdem gelten die Anmerkung zu 10.8.
12.4.1 Kontrolle von Software im Betrieb 12.4.3 Zugangskontrolle zu Quellcode	Quell- und Programmcode müssen während der Entwicklung geschützt werden, insbesondere beim Übergang vom Entwicklungs- über das Test- ins Produktivsystem. Im Betrieb muss der Programmcode geschützt werden.
12.4.2 Sicherheit von Testdaten	Falls betriebliche Daten im Test verwendet werden, müssen diese dabei besonders geschützt werden.

12.5 Sicherheit bei Entwicklungs- und Unterstützungsprozessen 12.5.2 Kontrolle nach Änderungen am Betriebssystem	Änderungen am Betriebssystem sowie die notwendigen Nacharbeiten gehören prinzipiell zum IT Betrieb.
12.5.3 Änderungen an Softwarepaketen	Bezieht sich auf die Änderung an Softwarepaketen, die von externen Anbietern geliefert werden. Sollten grundsätzlich sparsam verwendet werden.
12.5.4 Ungewollte Preisgabe von Informationen	Betriebliche Anwendungen von externen Lieferanten sollten – im Betrieb – auf unerwarteten Datenabfluss (Hintertüren) oder unsichere Datenspeicherung und –übertragung getestet werden.
12.5.5 Ausgelagerte Softwareentwicklung	Stellt eine Detaillierung von Punkt 10.2 dar, bei der es speziell um externe Softwareentwicklung geht.
12.6.1 Kontrolle technischer Schwachstellen	Hierunter versteckt sich u.a. der wichtige Sicherheitsprozess „Patch Management“. Für die Entwicklung und Wartung selbst entwickelter Software ergibt sich hieraus aber der Bedarf an einem Sicherheitssupport, der sehr kurzfristig Patches für bekanntgewordene Schwachstellen entwickelt und bereitstellt.
13 Umgang mit Informationssicherheitsvorfällen 14 Sicherstellung des Geschäftsbetriebs 15 Einhaltung von Vorgaben	Diese Prozesse beziehen sich zwar u.a. auch auf betriebliche Anwendungen, werden aber hier nicht vertieft behandelt, weil diese im ITIL wesentlich breiter behandelt werden.

Sicherheit Betrieblicher Anwendungssysteme im IT Service Management

Zur Auswahl Zu Untersuchender Prozesse

Entwicklung, Einführung und Betrieb betrieblicher Anwendungssysteme werden grundsätzlich in mehr oder weniger formalisierten Prozessen organisiert. Viele Unternehmen definieren diese Prozesse nicht grundlegend selbst, sondern nutzen ein Prozessframework als Vorlage. Besondere Bedeutung hat ITIL erlangt, das als Sammlung von Best Practices erwiesenermaßen praktisch erfolgreiche Prozesse miteinander kombiniert.

Im Folgenden sollen Prozesse, die im Lebenszyklus betrieblicher Anwendungssysteme eine Rolle spielen, auf die Messbarkeit von Sicherheitsqualität untersucht werden. Dazu könnten konkrete Prozesse in Unternehmen erfasst und analysiert werden; hier soll jedoch ein anderer Weg gewählt werden. Leider ist es schlechterdings unmöglich, die Gesamtheit in der Praxis vorkommender individueller ITSM-Prozesse zu erfassen. Eine empirische Analyse wäre deshalb entweder mit unverhältnismäßig großem Aufwand verbunden oder auf Einzelfälle beschränkt, deren Repräsentativität nicht feststellbar wäre.

Es bietet sich daher an, mit den ITIL-Prozessen die verbreitetesten Prozesse des IT Service Management auf diesen Aspekt hin zu untersuchen. Bei ihnen handelt es sich um bewährte Vorgehensweisen, die in vielen Fällen erfolgreich eingesetzt werden und die seit nunmehr zwei Jahrzehnten kontinuierlich den Rückmeldungen aus der Praxis und den technischen Entwicklungen angepasst werden.

Die ITIL-Kernveröffentlichungen des *Office of Government Commerce* nehmen vielfach Stellung zur Messbarkeit und zur Messung der Prozessqualität. Einige dieser Vorschläge haben Sicherheitsrelevanz – nicht nur jene zur Messung des ITIL-Prozesses *Information Security Management*, sondern auch solche zur Messung vieler anderer Prozesse, die in ihrer Gesamtheit den kompletten Lebenszyklus eines Anwendungssystems betreffen. Im Folgenden werden diese Empfehlungen aus der Sicherheitsperspektive betrachtet. Eine besondere Rolle nehmen dabei die Entwicklungs- und Testphase der Applikation ein, da ITIL diese zwar mit Prozessen wie *Release Management* und *Configuration Management* unterstützt, aber kein eigenes Vorgehensmodell für Softwareentwicklungsprojekte enthält. Die Projektmanagementmethode des OGC hat nicht dieselbe weite Verbreitung wie ITIL gefunden. Für diese Lebenszyklusphasen kommt daher den ISO-Normen 2700x (Kapitel „Sicherheitsanforderungen Für Betriebliche Anwendungssysteme Nach ISO 27002”) sowie den Methoden und Vorgehensweisen des Software Engineering (Kapitel „Sicherheit bei der Herstellung betrieblicher Anwendungssysteme”) ein spezieller Stellenwert zu.

Service Level Management

Vor der Einführung eines neuen IT-Service werden die Kundenanforderungen aufgenommen, analysiert und dokumentiert. Neben den funktionalen und nichtfunktionalen Anforderungen an die betriebliche Applikation werden dabei auch die Anforderungen an ihren Betrieb und den Support definiert. ITIL kennt dafür den Prozess des *Service Level Management* (OGC 2007b, S. 65ff.). In Zusammenarbeit mit dem Kunden wird der Service gestaltet; standardisierte Services werden aus einem Servicekatalog abgerufen. Neben vielen anderen Parametern wird dabei nach Kundenanforderung auch das

erforderliche Sicherheitsniveau festgelegt. ITIL schlägt zur Messung der Prozessqualität Kennzahlen vor (Ebel 2008, S. 225f.), von denen viele vor allem die Services als Output der Prozesse messen.

- Dazu zählen im Fall des *Service Level Management* die relative und absolute Häufigkeit von Service-Level-Verletzungen, was zunächst wenig Sicherheitsbezug zu haben scheint. An anderer Stelle fordert ITIL aber die besondere Erfassung von sicherheitsrelevanten Service-Level-Verletzungen. Es ist nur ein kleiner Schritt, die Kennzahlen zu Service-Level-Verletzungen ebenfalls separat für solche Fälle zu ermitteln, dann werden sie auch aus Sicherheitsperspektive relevant. Insbesondere ihre Entwicklung über mehrere Betrachtungsperioden gibt dann eine recht genaue Einschätzung, wie sich die Sicherheitsqualität entwickelt.
- Auch die Analyse, welche Service-Level-Verletzungen in welcher Häufigkeit auf Fehler von Subauftragnehmern zurückzuführen sind, gewinnt Relevanz für die Erhöhung des Sicherheitsniveaus, wenn die zusätzliche Kennzeichnung der Service-Level-Verletzungen als sicherheitsrelevant mit ausgewertet wird. Eine sich daraus unmittelbar ergebende Handlungsempfehlung könnte der Wechsel des Subauftragnehmers sein.
- Eine weitere ITIL-Kennzahl zum *Service Level Management* ist der Anteil der Services, für die es überhaupt keine SLA gibt, die also am offiziellen Prozess vorbei erbracht werden. Offensichtlich ist für Services ohne SLA auch kein Sicherheitsniveau definiert, das vom Kunden eingefordert werden könnte. Ihre Zahl sollte möglichst gering sein, was gleichbedeutend damit ist, für diese „Abdeckungsrate" des *Service Level Management* 100 Prozent als Zielgröße anzustreben. Sie hat somit zumindest zum Teil Sicherheitsbedeutung.
- Die Qualität des SLM-Prozesses kann darüber hinaus gemessen werden, indem man die Anzahl der SLA-Reviews und die der daraus abgeleiteten Maßnahmen analysiert. Damit wird deutlich, ob der Prozess „gelebt" wird, ob, wie schnell und in welchem Umfang also Änderungen der Kundenanforderungen oder neue Anforderungen vom SLM aufgegriffen werden. Auch dies betrifft mit allen anderen Anforderungen insbesondere die Sicherheitsanforderungen. Diese Kennzahl hat für sich alleine zwar keinen direkten Sicherheitsbezug, gibt aber Auskunft über die Aussagekraft der anderen erhobenen Kennzahlen.
- Über diese Kennzahlen hinaus sieht ITIL Kundenbefragungen zur Zufriedenheit mit dem SLM vor. Fragen zur Auswertung der Kundenzufriedenheit mit der Sicherheitsqualität könnten etwa lauten: Sind die Sicherheitsanforderungen an den IT Service mit Ihnen seitens des Service Providers zu Ihrer Zufriedenheit erörtert worden? Wurden Ihnen Alternativen aufgezeigt? Wurden Ihnen die Kosten dieser Alternativen genannt? Würden Sie die sicherheitsrelevanten Anforderungen in den SLA wieder genauso definieren? Sind die in den SLA mit Ihnen vereinbarten Sicherheitsanforderungen vom Service Provider in vollem Umfang erfüllt worden?

Availability Management

Zentrale Bedeutung bei der Einhaltung von SLA kommt der Verfügbarkeit der Services zu, um die sich der ITIL-Prozess *Availability Management* von der Definition der Verfügbarkeitsanforderungen bis zur Überwachung der tatsächlichen Verfügbarkeit kümmert (OGC 2007b, S. 97ff.). Zwischen Verfügbarkeit und Informationssicherheit besteht eine gegenseitige Abhängigkeit:

- Aus Sicherheitsperspektive setzt sich Informationssicherheit zusammen aus Vertraulichkeit, Integrität und Verfügbarkeit von Informationen
- Aus der Perspektive des *Availability Management* ist die Sicherheit einer von vielen Faktoren, die die Verfügbarkeit bedingen. Andere sind z.B. Redundanz, Hardwareersatzteillager, aktuelle und gepflegte Konfigurationsdaten.

Selbstverständlich müssen Sicherheitsmaßnahmen auf die vereinbarte Verfügbarkeit abgestimmt werden. Ein niedriges Sicherheitsniveau impliziert ein gesteigertes Risiko ungeplanter Serviceausfälle aufgrund von Sicherheitszwischenfällen. Dieses wiederum senkt die maximale Verfügbarkeit, zu der sich der Service Provider in einem SLA verpflichten kann.

Die Messung der Leistungsfähigkeit dieses Prozesses gibt leider recht wenig für die prozessbasierte Messung der Sicherheitsqualität her. Die wichtigsten KPI sind die Verfügbarkeiten der Services und der zu ihrer Erbringung verwendeten Komponenten sowie die zur Wiederherstellung eines Service nach einem Ausfall im Mittel benötigte Zeit. Auch hier gibt es natürlich einen Zusammenhang zur Sicherheitsqualität. Er lässt sich aber nicht isolieren, es sei denn, man wollte eine theoretische Verfügbarkeit bei Vernachlässigung nicht sicherheitsinduzierter Ausfälle konstruieren. Eine solche Kennzahl wäre nicht nur sehr weit hergeholt, sie mäße auch nicht primär den Prozess selbst, sondern seinen Output und erfüllte damit eben nicht den eingangs erhobenen Anspruch der prozessorientierten Messung von Sicherheitsqualität. Gleiches gilt für den Versuch, Wiederherstellungszeiten nach sicherheitsrelevanten Zwischenfällen zu isolieren. Schließlich hängt die Wiederherstellungszeit nach einem Ausfall von technischen und organisatorischen Faktoren ab, nicht primär vom Grund des Ausfalls.

IT Service Continuity Management

Der Prozess *IT Service Continuity Management* kümmert sich um Katastrophenfälle. Er soll das Risiko bestimmter katastrophaler Ereignisse vermindern und die Organisation auf den Fall vorbereiten, daß sie dennoch eintreffen. Neben Ereignissen wie Erdbeben, Feuer oder Hochwasser können auch manche sicherheitsrelevante

Angriffe zu berücksichtigen sein (OGC 2007b, S. 125ff.). ITIL schlägt zur Messung prozessbasierte Maßstäbe vor:

- Der Anteil der Service Level Agreements, die auf Katastrophenschutz Bezug nehmen. Damit wird gemessen, wie weit der Service Continuity-Gedanke die Organisation durchdrungen hat. In leicht abgeänderter Form könnte man messen: "Welcher Anteil der SLA nimmt Bezug auf die Vorbeugung und Notfallplanung für Katastrophenfälle durch interne oder externe Angriffe?"
- Die Anzahl der Audits im Zeitverlauf und der Anteil der erfolgreichen Audits misst, wie sehr der Prozess "gelebt" wird und wie gut die Organisation auf den Katastrophenfall vorbereitet ist. Eine Eingrenzung nach Katastrophen durch Angriffe ist auch hier möglich und gäbe der Kennzahl zusätzliche Sicherheitsbedeutung.

Supplier Management
Die Lieferanten und Subunternehmer, die der Service Provider engagiert, um mit ihrer Unterstützung seine Serviceversprechen zu halten, bestimmen die Qualität der Services ebenso wie er selbst. Mit Ihrer Auswahl und der Pflege der Lieferantenbeziehungen beschäftigt sich der Prozess *Supplier Management* (OGC 2007b, S. 149ff.). Da eine von einem Zulieferer verursachte Sicherheitslücke ebenso folgenschwer wie eine selbstverschuldete sein kann, die Kontrolle und Steuerung sich aber schwieriger als bei eigenen Mitarbeitern gestalten, ist auch dieser Prozess sicherheitsrelevant.

Die Qualität des *Supplier Management* wird gemessen, indem man die Abdeckung der Lieferantenbasis durch gemäß diesem Prozess verwaltete Beziehungen oder die Anzahl und Entwicklung der Lieferantenreviews erhebt. Primär den Output des Prozesses messen Anzahl, Anteil und Entwicklung der von Lieferanten verschuldeten SL-Verletzungen. Letzteres ließe sich dank separater Erfassung sicherheitsrelevanter SL-Verletzungen auch sicherheitsbezogen spezialisieren.

Information Security Management
Der ISM Prozess ist der ITIL-Prozess, der Sicherheit im Namen trägt und der unmittelbar für Sicherheit zuständig ist. ITIL beschreibt nicht technische Lösungen, sondern die sie verwendende Ablauforganisation (OGC 2007b, S.141ff.).

Zur Messung der Prozessqualität wird z.B. vorgeschlagen, die Menge der Angriffe und Infektionen im Zeitverlauf zu erfassen. Dieser Kennwert misst allerdings sowohl die Qualität ihrer Erkennung (je mehr desto besser) als auch die Qualität der Vorbeugung (je weniger, desto besser) und ist damit insgesamt wenig aussagekräftig.

Weitere in diesem Zusammenhang vorgeschlagene Kennzahlen sind auch in der Sicherheitsbranche bekannt aber in vielen Fällen nicht prozessbasiert. Der ISM-Prozess als solcher ist in ITIL allerdings so allgemein formuliert, dass es schwierig ist, ihn anhand von Kennzahlen zu messen. Anhaltspunkte, die dennoch dafür sinnvoll sein könnten, sind z.B. die Frequenz der Überarbeitung von Richtlinien, Analysen und Evaluationen.

Change Management
Sämtliche Änderungen an der Infrastruktur haben definierte Prozesse zu durchlaufen. Im Rahmen des *Change Management* wird über sie entschieden (OGC 2007a, S. 42ff.). Zu den Prüfungen, denen eine potentielle Änderung im Genehmigungsprozess unterzogen wird, gehören auch solche, die ihre Konsequenzen für die Angriffssicherheit der Infrastruktur abschätzen. Nur ein konsequent umgesetzter Change Management Prozess bietet einen wirksamen Schutz vor unbedacht aufgerissenen Sicherheitslücken in der Infrastruktur. Um ihn zu messen, kann man seinen Abdeckungsgrad erheben, also die Anzahl der nicht genehmigten Änderungen, die im Idealfall Null sein sollte. Mit der Anzahl der Störungen, die unmittelbar durch Änderungen verursacht wurden, misst man die Sorgsamkeit des Genehmigungsprozesses (Ebel 2008, S. 394). Zum wiederholten Mal zahlt sich hierbei die Kennzeichnung von Störungen als sicherheitsrelevant aus, wenn man den Sicherheitsbeitrag des Prozesses zu erfassen beabsichtigt.

Event Management, Incident Management und Problem Management
Drei Prozesse sorgen für einen möglichst reibungslosen Systembetrieb. *Incident Management* befasst sich mit der Behandlung von Störungen, (OGC 2007c, S. 46ff.) *Problem Management* mit den hinter den Störungen liegenden Ursachen (OGC 2007c, S. 58ff.) und *Event Management* mit Vorfällen, z.B. aus automatisiertem Monitoring, die ein Eingreifen erforderlich machen (OGC 2007c, S.35ff.). Die Prozesse arbeiten eng zusammen und können alle drei auch sicherheitsrelevante Fälle betreffen. Ein Event kann ein Hinweis auf einen Systemeinbruchsversuch sein, ein Incident kann aus einem erfolgreichen Systemeinbruch resultieren, ein Problem kann eine offene Sicherheitslücke sein, die diesen Systemeinbruch ermöglicht. Erkennt man sicherheitsrelevante Events, Störungen und Probleme als solche und kennzeichnet man sie für die spätere Auswertung als solche, so kann man nicht nur an ihrer Anzahl, Erfolgsquote, Bearbeitungsdauer und Entwicklung im Zeitverlauf den Sicherheitsbeitrag dieser operativen Prozesse messen. Die erhobenen Daten liefern auch das Material zur Messung anderer Prozesse, wie bereits beschrieben wurde.

Weitere Prozesse
Weitere Prozesse zu Erstellung, Inbetriebnahme und Betrieb betrieblicher Anwendungssysteme haben mittelbare Sicherheitsrelevanz. So definiert das *Capacity Management* Kapazitätsanforderungen, die bei der Definition von Sicherheitsmaßnahmen zu berücksichtigen sind.

Der *Demand Management* Prozess sorgt u.a. dafür, dass die Kundenorganisation ein Sicherheitskonzept bekommt, das ihren Anforderungen entspricht und berät bei technischen Fragen. Der Prozess *Release Management* kümmert sich u.a. um die Verteilung von Sicherheitspatches auf die Client-PCs der Mitarbeiter. Das *Service Asset and Configuration Management* dokumentiert die aus Hardware, Software und Dokumenten bestehende Konfiguration. Seine gewissenhafte Durchführung ist Grundlage praktisch aller anderen Prozesse eines IT Service Providers und damit auch der oben aufgeführten.

Diese Prozesse zur Messung von Sicherheit heranzuziehen, ist möglich, aber u.E. wenig zweckdienlich, da sie Sicherheit entweder nur mittelbar betreffen oder diese nur einen kleineren Teil ihrer Aufgabe ausmacht.

Sicherheit bei der Herstellung Betrieblicher Anwendungssysteme

Projekt Kick-Of
Zum Start eines Softwareentwicklungsprojekts oder eines neuen Software-Releases gehören neben der allgemeinen Projektplanung auch der Aufbau des Entwicklungsteams und die Festlegung des Entwicklungsprozesses. Hierzu gehören auch die sicherheitsrelevanten Punkte

- Sicherheits- und Qualitätsanforderungen an externe Mitarbeiter
- Anforderungen von Räumen und IT-Ressourcen sowie die Vergabe der notwendigen Zugangs-, Zutritts- und Zugriffsrechte für interne und externe Mitarbeiter, idealerweise nach einem formalen, dokumentierten Verfahren, das zum Projektabschluss auch die Zurücknahme der Rechte erlaubt (vgl. „Projektabschluss")
- Ggfs. Einrichtung von Sicherheitszonen oder speziellen Büros, Räumen und Einrichtungen und die entsprechenden Zutrittsrechte
- Prozess zur Überwachung der (internen und) externen Mitarbeiter sowie zur Überprüfung von deren Leistungen
- Prozesse zur Verwaltung von Quellcodes und Programmcodes sowie Dokumentation, speziell zur Gewährleistung der Integrität bei der Übergabe zwischen Entwicklungs-, Test- und Produktivsystemen. Diese Prozesse können sich je nach der Sicherheitsrelevanz der zu entwickelnden Software deutlich unterscheiden.

Mit der Gewährleistung der Integrität der Quell- und Programmcodes kann sowohl eine Manipulation des Codes durch Dritte als auch eine Infektion mit Schadcode ausgeschlossen werden. Natürlich sind auch die Vertraulichkeit und Verfügbarkeit von Code sicherheitsrelevant, aber hier nur von untergeordneter Bedeutung. Dasselbe gilt für die Versionierung, die zwar innerhalb des Entwicklungsprozesses wichtig ist, aber nicht in Bezug auf die Sicherheit.

Im Rahmen eines einzelnen Projektes scheinen Kennzahlen in Bezug auf diese Aufgaben nicht zweckmäßig zu sein. Sofern aber innerhalb des Unternehmens eine Vielzahl solcher Projekte durchgeführt wird, können Kennzahlen definiert werden, die jeweils die Anzahl oder den Anteil an Projekten angeben, in denen der entsprechende Punkt nicht berücksichtigt wurde.

Im Zusammenhang mit der Sicherheit von Quell- und Programmcodes können außerdem Kennzahlen des *Incident Management* verwendet werden, z.B. die Anzahl von Sicherheitsvorfällen in Folge fehlerhaften Codes.

Analyse und Design
Zur Analysephase innerhalb eines Softwareentwicklungsprojektes gehören alle Überlegungen und Festlegungen, die eine generelle Bedeutung für das System haben und nicht auf der Basis technischer Überlegungen erledigt werden können. Aus Sicherheitssicht sind dies:

- Benutzerkreis für die Anwendung: Nur interne Benutzer / Partner des Unternehmens / öffentlicher Zugriff
- Art der von der Anwendung verarbeiteten Daten, speziell im Hinblick auf eine notwendige Klassifizierung der Daten
- Geschäftliche Bedeutung der Anwendung und der verarbeiteten Daten
- Art der Benutzerverwaltung: Registrierung, Rechtevergabe, Sonderrechte, Passwörter
- Bedarf an einer funktionalen Trennung bestimmter Verantwortlichkeiten (Separation of Duties)
- Bedarf an Kommunikationsmechanismen wie elektronische Nachrichten oder externe Zugriffe, die eine Verschlüsselung erfordern

In der Designphase sind die Ergebnisse der Analysephase aufzugreifen und außerdem weitere Punkte zu berücksichtigen, die soweit technischer Natur sind, dass sie für die Analyse nicht relevant waren. Technische Entscheidungen der Designphase betreffen die folgenden Punkte:

- Backup-freundliche Datenspeicherung oder Bereitstellung spezieller Backup-Mechanismen
- Erzeugung von Auditprotokollen (Benutzer-, Administrations- und Fehlerprotokolle) der Anwendung, die Datenschutz-konform gespeichert und ausgewertet werden können. Idealerweise unterstützt die Anwendung die elektronische Auswertung und ggfs. die Anonymisierung oder Pseudonymisierung der Protokolle.
- Sicherheitsmechanismen nach Kapitel 12.2 des ISO 27002: Überprüfung von Ein- und Ausgabedaten, Kontrolle der internen Verarbeitung sowie Gewährleistung der Integrität von Nachrichten.

Alle Sicherheitsanforderungen sind dabei als „sicherheitsrelevant" zu dokumentieren. Als Kennzahl schlagen wir die Anzahl sicherheitsrelevanter Anforderungen vor.

Dies dokumentiert einerseits die Durchführung des Prozesses, andererseits – wenn auch nur sehr grob – den Prozessoutput. Vorteilhaft ist, dass diese Kennzahl als Benchmark dienen kann für den Anteil nicht oder fehlerhaft umgesetzter Sicherheitsanforderungen (vgl. „Test" und „Support"). Detailliertere Kennzahlen wären außerdem nach Ansicht der Autoren für Managementebenen nicht verständlich.

Softwareentwicklung
Getreu des Paradigmas, dass nach sorgfältigen Analyse- und Designphasen in der Entwicklung praktisch keine Freiheitsgrade mehr bestehen, bestehen keine zusätzlichen Sicherheitsanforderungen für die eigentliche Softwareentwicklung.

Da es aber üblich ist, dass einzelne Anforderungen während der Entwicklung aus Gründen von Zeit und Aufwand wieder gekippt oder zumindest zurückgestellt werden, ist es sinnvoll, die Anzahl und den Anteil (in %) der nicht implementierten Sicherheitsanforderungen als Kennzahlen zu verwenden.

Test
Grundsätzlich kann sorgfältiges Softwaretesten die Qualität und die Sicherheit von Software massiv erhöhen. Zum allgemeinen Thema „Testing" wurden aber bereits seit vielen Jahren zahlreiche Arbeiten verfasst (Myers 2001, Sommerville 2011), so dass wir dieses Thema hier nicht allgemein vertiefen wollen.

Die (weiteren) sicherheitsrelevanten Aspekte des Softwaretests entsprechen den Punkten 12.2.1 bis 12.2.4 sowie 12.4.1 bis 12.4.3 und – falls externe Mitarbeiter beteiligt sind – den Punkten 6.2, 10.2 und 12.5.5 des ISO 27002 (vgl. „Sicherheitsanforderungen Für Betriebliche Anwendungssysteme Nach ISO 27002"). Im Testprozess betrifft dies die folgenden Schritte

Tabelle 2: Kennzahlen für Softwaretests

Prozessschritte	**Mögliche Kennzahlen**
Sicherstellen der Zuverlässigkeit und Qualität externer Mitarbeiter (falls zutreffend)	▪ Anzahl der beteiligten externen Mitarbeiter ▪ Anteil der nicht bekannten / geprüften Personen
Übernahme der zu testenden Programmmodule aus der Entwicklungsumgebung und Prüfung, dass die Module unverändert übernommen wurden (Integrität)	▪ Anteil der ohne Integritätsprüfung übernommenen Module (in %) ▪ Anteil der fehlgeschlagenen Prüfungen (in %)
Generierung oder Übernahme von Testdaten und Testfällen. Falls hierbei produktive Daten verwendet werden Genehmigung und besonderer Schutz	▪ Anteil der Testabläufe, bei denen Produktivdaten verwendet wurden (in %) ▪ davon Anteil ohne Genehmigung oder besonderen Schutz
Durchführung von Sicherheitstests nach 12.2.1 bis 12.2.4 des ISO 27002	▪ Anteil von Tests, bei denen auf die Sicherheitstests verzichtet wurde (in %) ▪ Anteil von Tests, bei denen die Sicherheitstests fehlgeschlagen sind (in %) ▪ Anteil an Sicherheitsanforderungen (vgl. „Softwareentwicklung"), die nicht verifiziert werden konnten
Durchführung weiterer funktionaler und nichtfunktionaler Tests (entsprechend dem oben stehenden Absatz nicht im Scope unserer Betrachtungen)	
Behandlung der Testergebnisse und ggfs. unveränderte Weitergabe der getesteten Programmmodule	Hängt von der konkreten Ausgestaltung des Prozesses ab.

Support
Der Sicherheitssupport für in Betrieb genommene Anwendungen hat die Aufgabe, bekanntgewordene Sicherheitslücken möglichst schnell zu schließen, indem Patches bereitgestellt werden, die dann dem ITIL Prozess *Change Management* zur Verfügung gestellt werden, damit sie in die Produktivsysteme eingespielt werden.
Mögliche Kennzahlen hierzu wären

- Bedarf an Patches pro Jahr (absolute Anzahl)
- Anteil an Patches, die nicht in einem vorgegebenen Zeitraum zur Verfügung stehen (in %)
- Anteil an Patches, die im Systemtest oder im Produktivsystem Probleme bereiten (in %)

Weitergehender Support im Sinne der Bereitstellung zusätzlicher Softwarefunktionen stellt keine Sicherheitsaufgabe dar, ist also hier nicht zu betrachten.

Projektabschluss
Zum Projektabschluss, der in der klassischen Softwareentwicklung verschiedene interessante Punkte enthält, gehört aus Sicherheitssicht auch

- Das De-Provisioning bzw. die Zurücknahme spezieller Zugangs-, Zutritts- und Zugriffsrechte für interne und externe Mitarbeiter

Wenn die Vergabe der Rechte durchgängig nach einem formalen Prozess durchgeführt wurde, sollte dies auch für die Zurücknahme der Rechte gelten. Innerhalb eines einzelnen Prozesses erscheint eine Kennzahl, die über ein „wurde durchgeführt / wurde nicht durchgeführt" hinausgeht, nicht zweckmäßig. Über viele Prozesse eines Unternehmens hinweg ist – analog zu „Projekt Kick-Off" – eine Kennzahl denkbar, die die Anzahl oder den Anteil der Prozesse ohne explizite Zurücknahme von Rechten angibt.

ZUSAMMENFASSUNG UND AUSBLICK

Es zeigt sich, dass die Sicherheit von Applikationen auch abseits von großen Anhäufungen technischer Parameter messbar ist, wenn man nicht nur die Hard- und Softwarekomponenten, sondern auch die Qualität der sicherheitsunterstützenden Prozesse ins Auge fasst. Man misst dann nicht mehr nur das Erreichen eines Zieles, sondern auch, wie gut es verfolgt wurde.

Bezüglich einiger IT-Service-Management-Prozesse hat sich ein recht einfaches Muster wiederholt:

- Man misst den Abdeckungsgrad eines sicherheitsrelevanten Prozesses. Die Zielgröße ist 100%.
- Berücksichtigt man bei der Datenerfassung die Sicherheitsrelevanz, erfasst man also z.B. sicherheitsrelevante Störungen oder sicherheitsrelevante SLA-Klauseln separat, so ist es ein Leichtes, gängigen Kennzahlen zur Messung der Prozessqualität ihre Pendants zur Seite zu stellen, die über den Sicherheitsbeitrag des jeweiligen Prozesses Auskunft geben.

Die Autoren sprechen sich dafür aus, prozessorientierte Kennzahlen zur Messung der Sicherheit heranzuziehen. Da das Informationsbedürfnis auf verschiedenen Hierarchieebenen unterschiedlich ist, ersetzen diese aber technische Sicherheitsparameter nicht. Technische Größen behalten ihre Wichtigkeit insbesondere für die Analyse von Einzelfällen und die Erarbeitung technischer Verbesserungsmaßnahmen durch Sicherheitsverantwortliche der IT. Sie eignen sich aber weit schlechter als prozessorientierte Kennzahlen als strategisches Instrument der Unternehmensführung auf den darüber liegenden Hierarchieebenen.

AKTUELLE ENTWICKLUNGEN

Da in den letzten Jahren kein neuer ITIL-Standard veröffentlicht wurde – aktuell ist immer noch der ITIL-Standard V3 von 2007 – beschränkt sich unsere Betrachtung der Entwicklungen hier auf die Entwicklung der ISO 27xxx Standardfamilie.

Der Messbarkeit der Informationssicherheit wird in den Standardsierungsgremien mehr und mehr Bedeutung zugerechnet. Dabei gehen die aktuellen Ansätze dahin, Metriken prozessorientiert zu bilden und in einem PDCA-Zyklus zu managen (ISO/IEC 2011, ISO/IEC 2013). Dieser Ansatz entspricht den gängigen Mechanismen auch zum Management der Informationssicherheit selbst und steht nicht im Widerspruch zu den dargestellten Vorschlägen dieser Arbeit.

Für die Bildung der Metriken selbst ist aber immer noch wenig Hilfestellung vorhanden. Der Ansatz der Autoren, wonach Sicherheitsmetriken – zumindest für betriebliche Anwendungssysteme – entlang deren Lebenszyklusprozesse gebildet werden sollten, könnte damit die noch offenen Aufgaben zur Bildung der notwendigen Sicherheitsmetriken unterstützen.

LITERATURVERZEICHNIS

BSI (Hrsg.). 2008. *IT-Grundschutz-Kataloge, M 2.193: Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit.* https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m02/m02193.html, Abruf am 29.06.2011

DIN. 2008a. *DIN ISO/IEC 27001: Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC 27001:2005)*

DIN. 2008b. *DIN ISO/IEC 27002: Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Informations-Sicherheitsmanagement (ISO/IEC 27002: 2005)*

Drucker, P.F. 1974. *Management*. New York, 5. Auflage

Ebel, N. 2008. *ITIL-V3-Basis-Zertifizierung*, Addison-Wesley, München

Funk, W. 2011. *Rollen für Informationssicherheit in einer Best-Practice-Organisation*. The Bulletin Security Management, BSM Anwender Nr. 202-1.0, http://www. security-management.de/de/publikationen/20100109_BSM_Anwender_202_1.0_Rollen_Informationssicherheit.pdf, Abruf am 29.06.2011

ISO/IEC. 2009. ISO/IEC 27004*:2009 Information technology. Security techniques. Information security management. Measurement*

ISO/IEC. 2011. *ISO27001 Security*: *ISO/IEC 27004*, http://www. iso27001security.com/html/27004.html, abgerufen am 21.06.2011

ISO/IEC. 2013. *ISO27034 Information Technology – Security Techniques – Application Security*: http://www.iso27001security.com/html/27034.html, abgerufen am 24.06.2013

Jaquith, A. 2007. *Security Metrics – Replacing Fear, Uncertainty, and Doubt*, Addison-Wesley, Amsterdam

Myers, G.J. 2001. *Methodisches Testen von Programmen*, Oldenbourg, München

OGC (Hrsg.). 2007a. *Service Transition: ITIL*, TSO, London

OGC (Hrsg.). 2007b. *Service Design: ITIL*, TSO, London

OGC (Hrsg.). 2007c. *Service Operation: ITIL*, TSO, London

Röckle, H. und Dorrhauer, C. 2011. *Messbarkeit der Sicherheitsqualität im Lebenszyklus betrieblicher Anwendungssysteme*, in: Herausforderungen an die Wirtschaftsinformatik: Betriebliche Anwendungssysteme, News & Media, Berlin, S. 155-174

Schimpf, G. und Röckle, H. 2009. *Security Reporting in großen Unternehmen*, in: Horster, P./ Schartner, P. (Hrsg.) D.A.CH Security 2009, syssec, S. 240-252

Sommerville, I. 2011. *Software Engineering*, Boston, Pearson