Dirk Fox, Kai Jendrian

Struktur von Sicherheitsrichtlinien

Sicherheitsrichtlinien sind ein wichtiges Instrument der Informationssicherheit. Dennoch sucht man in Standards vergeblich nach Empfehlungen für deren Aufbau und Strukturierung. Der vorliegende Beitrag versucht Abhilfe.

1 Hintergrund

Die Erstellung und Inkraftsetzung von Sicherheitsrichtlinien sind wesentlicher Bestandteil eines wirksamen Sicherheitsmanagements. Folgerichtig fehlt in keinem etablierten Standard die Forderung nach einem Regelwerk für Informationssicherheit. So enthalten beispielsweise die Maßnahmenkataloge des IT-Grundschutzes zahlreiche Empfehlungen für verschiedene Regelungsbereiche.

Auch über die hierarchische Gliederung und den Wesensgehalt der Regelwerke herrscht – abgesehen von der Namensgebung – in Literatur und Praxis weitgehend Einigkeit.

Die Regelungsdokumente auf den verschiedenen Ebenen der häufig zur Veranschaulichung herangezogenen Regelwerkspyramide (siehe Abb. 1) sollen dabei Antworten auf die folgenden Fragen liefern:

- Warum ist Informationssicherheit für die Organisation wichtig?
- Was sind die speziellen Anforderungen an den Informationsschutz?
- Wie sollen die Anforderungen konkret umgesetzt werden?
- Wie wurden die Anforderungen tatsächlich umgesetzt?

An oberster Stelle steht dabei eine „Sicherheitspolitik" (Strategische Sicherheitsziele und deren Einordnung in die Unternehmensphilosophie), gefolgt von „Sicherheitsrichtlinien", die Anforderungen an den Informationsschutz für unterschiedliche Bereiche formulieren. In Sicherheitsanweisungen, -konzepten und -standards werden dann konkrete Vorgaben festgelegt, deren Umsetzung schließlich auf der Ebene der Sicherheitsdokumentation als Fundament der Pyramide beschrieben wird. Sowohl die Vorgaben als auch die Dokumentationen enthalten in der Regel detaillierte technische Konfigurationen oder organisatorische Abläufe.

Vergeblich sucht man in Standards der Informationssicherheit jedoch nach einheitlichen Empfehlungen für den Aufbau von Richtlinien-Dokumenten: Welche Aspekte müssen darin geregelt werden? Welche Gliederung ist zu empfehlen? Welche begleitenden Dokumente sollten beigefügt werden?

Das Fehlen eines solchen Standards ist umso verwunderlicher, als die Eignung eines Sicherheitsregelwerks nicht allein von Regelungsinhalten, sondern ganz wesentlich von seinem Aufbau und der Vollständigkeit der Regelungsaspekte bestimmt wird: Wem hilft ein Notfallkonzept ohne Namen und gültige Kontaktdaten der Ansprechpartner? Wie kann der Adressat einer Regelung erkennen, dass sie ihn betrifft, wenn Zielgruppe und Geltungsbereich nicht klar festgelegt sind und die Aktualität des Dokuments nicht erkennbar ist?

Auch stellen sich in der Praxis immer wieder vermeintlich profane Fragen, z. B. wie mit Elementen in Richtlinien umgegangen werden soll, die einer ständigen Veränderung unterliegen, ohne dass jedes Mal ein kompletter Freigabeprozess durchlaufen werden muss.

In vielen Unternehmen werden Richtlinien „ad hoc" entworfen – ohne vereinheitlichte Struktur, ohne Berücksichtigung bereits verabschiedeter Richtlinien, ohne systematischen Aufbau. Das zwingt nicht nur den Adressaten, sich jeweils neu auf abweichende Strukturierungen einzustellen, sondern führt meist zu erheblichen Eignungsmängeln der resultierenden Regelungsdokumente in der Praxis, weil wichtige Aspekte fehlen oder die Richtlinien verwirren, schlimmstenfalls sogar widersprüchlich sind.

Dabei ist Abhilfe einfach: Durch einen geregelten Prozess zur Erstellung, Verabschiedung und Veröffentlichung von Regelungen – unterstützt durch eine einheitliche Dokumentenvorlage mit fester Struktur – lassen sich Verständlichkeit, Klarheit und Vollständigkeit entwickelter Richtlinien erheblich verbessern. Im Folgenden wird eine solche Struktur für Sicherheitsrichtlinien vorgeschlagen.

2 Richtlinien-Struktur

2.1 Titel

Allein die Wahl des Titels einer Richtlinie kann erheblichen Einfluss auf deren Wirksamkeit haben. Passt der Titel nicht oder ist er un- oder missverständlich, wird die Richtlinie möglicherweise nicht richtig wahrgenommen – und die darin enthaltenen Regelungen werden nicht beachtet.

Bei der Auswahl des Titels muss daher darauf geachtet werden, dass die Erwartung, die der Titel weckt, auch mit dem tatsächlichen Inhalt der Richtlinie übereinstimmt. Und auch die Umkehrung muss gelten: Wird ein Mitarbeiter, der ei-

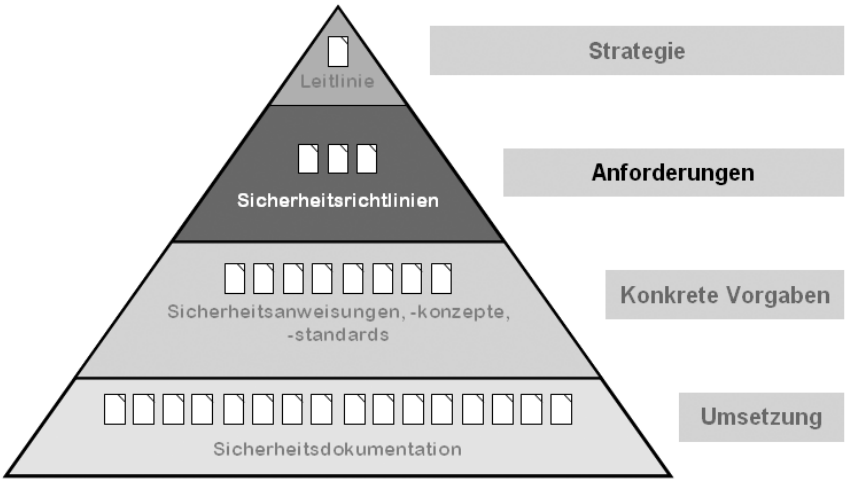
Kai Jendrian

Security Consultant bei der Secorvo Security Consulting GmbH, lizenzierter Auditor. Beratungsschwerpunkte: Infirmation Security Management, IT-Sicherheitspolicies.
E-Mail: kai.jendrian@secorvo.de

Dirk Fox

Geschäftsführer der Secorvo Security Consulting GmbH und Herausgeber der DuD.
E-Mail: dirk.fox@secorvo.de

Abbildung 1 |



ne der in der Richtlinie enthaltenen Regelung sucht, unter dem gewählten Titel das Gesuchte vermuten?

Idealerweise sollte dreierlei aus dem Titel hervorgehen:

- dass es sich um eine Richtlinie handelt (sofern das nicht bspw. aus einer speziellen Nummerierung oder anderen Dokumenteneigenschaften hervorgeht),
- welcher Sachverhalt darin geregelt wird und
- für wen die Richtlinie gilt (auch das kann durch eine spezielle Kennzeichnung oder andere formale Eigenschaften ausgedrückt werden).

Im Falle von langen oder komplizierten Titeln bietet es sich an, einen alternativen Kurztitel festzulegen, um diesen beispielsweise in Übersichten, aber auch in der Kopf- oder Fußzeile der Richtlinie nutzen zu können.

Abkürzungen und Fachbegriffe, deren Kenntnis nicht vorausgesetzt werden kann, sollten bei der Formulierung vermieden werden.

2.2 Motivation und Regelungsgegenstand

Die Einführung einer Richtlinie sollte nicht nur den Gegenstand der Regelung umreißen, sondern auch eine kurze Motivation umfassen. Sie sollte erläutern, was in der Richtlinie geregelt wird (z. B. der Umgang mit und die Wahl sicherer Passworte) und warum die Regelung getroffen wird.

Dabei kann sich die Motivation sowohl auf Grundsatzentscheidungen der Unternehmensleitung als auch auf aktuelle Entwicklungen oder konkrete externe oder interne Vorfälle beziehen. Die Erfahrung zeigt, dass besonders Verweise auf interne Vorfälle oder Anlässe geeignet sind, die Mitarbeiter zur Einhaltung von Regelungen anzuhalten: Niemand möchte dafür verantwortlich sein, dass sich ein Schadensereignis wiederholt.

2.3 Zielsetzung

Nur wenn das Ziel einer Richtlinie präzise festgelegt ist, lassen sich die gewählten Regelungen auf Vollständigkeit, Widerspruchsfreiheit und Angemessenheit überprüfen. Daher sollte eine klare Zieldefinition immer der erste Schritt bei der Entwicklung einer Richtlinie sein. Im Richtlinien-Dokument selbst dient sie zusätzlich der Motivation der getroffenen Regelungen und sorgt für Transparenz.

Tatsächlich ist eine präzise Zielfestlegung meist schwieriger, als auf den ersten Blick vermutet. So macht es hinsichtlich des Regelungsumfangs z. B. einen erheblichen Unterschied, ob man mit einer Passwort-Policy die Wahl hinreichend sicherer Passwörter erreichen möchte – oder einen wirksamen Schutz vor einem unberechtigten Login: Letzteres erfordert außer Anforderungen an die Passwort-Wahl auch Regelungen zum Umgang mit dem gewählten Passwort.

Auch aus übergeordneter Perspektive lohnt es, über die Zielsetzung genauer nachzudenken. Denn jeder Regelung sollte ein konkretes Risiko gegenüberstehen, das durch diese wirksam reduziert wird. Allzu oft stellt sich bei der Diskussion der Zielsetzung heraus, dass die zunächst vorgesehene Regelung unzureichend oder, schlimmer noch, ungeeignet ist, die erwünschte Risikoreduktion zu bewirken. Eine genaue Klärung der Zielsetzung hat daher häufig eine substantielle Verbesserung des Regelwerks zur Folge.

2.4 Zielgruppe

Sicherheitsrichtlinien werden zumeist bezogen auf ein konkretes, oft technisches[1] oder organisatorisches[2] Thema verfasst. Eine rein thematische Strukturierung von Richtlinien verkennt jedoch, dass zahlreiche Regelungsaspekte dieser Themen sehr unterschiedliche Zielgruppen ansprechen: Der IT-Nutzer muss wissen, welche Eigenschaften ein von ihm gewähltes Passwort aufweisen und wie er mit diesem Passwort umgehen muss, während der Passwortrücksetzungsprozess in erster Linie vom IT-Benutzerservice verinnerlicht sein sollte.

Werden Regeln für unterschiedliche Zielgruppen in einer Richtlinie zusammengefasst, leiden meist Verständlichkeit und Übersichtlichkeit: Jeder Leser muss die für ihn relevanten Regelungen herausfiltern – das ist nicht nur mühsam, sondern auch fehleranfällig.

Richtlinien sollten daher immer für exakt eine einzige, klar begrenzte Zielgruppe verfasst werden. In der Praxis wird es damit folgerichtig unterschiedliche Richtlinien zum selben Themenbereich geben: Eine Passwortrichtlinie für IT-Nutzer, eine zweite für Administratoren (mit höheren Anforderungen) und möglicherweise eine dritte für Externe, sowie Verfahrensanweisungen für den Benutzerservice und die Administratoren ausgewählter IT-Systeme.

Die Sicherheitsrichtlinien lassen sich dabei übersichtlich als Matrix darstellen, gegliedert nach Themenbereich und Zielgruppe. Dabei kommt es darauf an, dass die Betroffenen einfach feststellen können, welche Richtlinien für sie selbst bindend sind.

2.5 Geltungsbereich

Neben der Zielgruppe, für die eine Richtlinie relevant ist, ist der Geltungsbereich eine wichtige Begrenzung.

Dafür sind die folgenden Fragen zu klären: Gilt eine Richtlinie für alle Nutzer von IT-Systemen einschließlich externer

1 Z. B. „Passworte", „Backup", „Virenschutz" oder „Speichermedien"

2 Z. B. „Sicherheitsorganisation und -prozesse"

Mitarbeiter, Praktikanten und IT-Dienstleister? Gilt sie für alle IT-Systeme des Unternehmens oder auch für jedes IT-System, dass mit der IT-Infrastruktur des Unternehmens verbunden wird – einschließlich des Home-Office, eines Besucher-Laptops und des privaten USB-Sticks? Gilt sie nur für eine Einzelgesellschaft, eine Holding oder alle Tochterunternehmen? Gilt sie unternehmensweit oder nur für bestimmte Niederlassungen?

Aus dem Geltungsbereich leiten sich in der Regel auch eine geeignete Zuständigkeit für die Freigabe und konkrete Umsetzung der Richtlinie ab (siehe Abschnitt 2.7).

2.6 Regelungsinhalte

Die Regelungsinhalte selbst sollten übersichtlich, z. B. durch eine Hervorhebung von Kernsätzen dargestellt und mit jeweils einer kurzen, verständlichen Erläuterung versehen werden. Dabei sollten keine Fachtermini verwendet werden, deren Kenntnis bei der Zielgruppe nicht vorausgesetzt werden kann.

Eine Untergliederung in technische und organisatorische Maßnahmen kann ebenso sinnvoll sein wie eine Strukturierung nach Systemen (Betriebssystem) oder Systemklassen (Client- vs. Server-Systeme). Die Anzahl der Regelungen einer Richtlinie sollte überschaubar bleiben. Werden es zu viele, empfiehlt es sich meist, eine Aufteilung in mehrere Richtlinien vorzunehmen.

2.7 Umsetzung

Eine Regelung, die eine Änderung von Prozessen oder Abläufen bewirkt, kann nicht immer unmittelbar umgesetzt werden. Möglicherweise erfordert sie technische Umstellungen, die einen Übergang erfordern, oder ein fließender Wechsel ist aus organisatorischen Gründen wünschenswert. So wird man bei einer Verschärfung der Passwort-Anforderungen nicht unmittelbar alle bestehenden Accounts mit schwächeren Passwörtern deaktivieren, sondern die neuen Passworteigenschaften beim nächsten regulären Passwortwechsel verlangen.

Die für die Umsetzung der neuen Regelungen geltenden Fristen sind konkret festzulegen und ein geeigneter Verantwortlicher (ggf. der Nutzer selbst, Führungskräfte mit Personalverantwortung, ein Administrator etc.) zu benennen.

Schließlich sollte die Richtlinie auch die Überprüfung der Umsetzung regeln: Wie (Stichprobe? Audit?), wann (regelmäßig?) und durch wen (Vorgesetzter? IT-Revision?) wird sie geprüft? Wer ist dafür verantwortlich, wie wird das Ergebnis dokumentiert und an wen berichtet?

Dabei ist auch eine Festlegung der möglichen Konsequenzen bei Regelverstößen zu empfehlen, insbesondere dann, wenn diese über arbeitsrechtliche Maßnahmen hinausgehen, wie beispielsweise die Sperrung des Zugriffs einer betroffenen Niederlassung auf IT-Systeme der Zentrale oder der (möglicherweise nur temporäre) Entzug einer Berechtigung.

2.8 Gültigkeit

Üblicherweise wird in einer Richtlinie das Datum ihres Inkrafttretens angegeben. Aber auch wenn zum Zeitpunkt der Freigabe einer Richtlinie häufig noch nicht bekannt ist, wie lange diese Richtlinie gelten soll, ist es doch sinnvoll ein „Verfallsdatum" der Richtlinie festzulegen. Wird die Richlinie nicht vor diesem Zeitpunkt überprüft und für weiterhin notwendig erachtet, verliert sie zum angegebenen Zeitpunkt automatisch ihre Gültigkeit. Dadurch kann vermieden werden, dass jede Richtlinie formell außer Kraft gesetzt werden muss, damit sie nicht von irgend jemandem in 25 Jahren aus der Schublade gezogen wird – wenn sie wahrscheinlich schon lange nicht mehr aktuell ist.

Zusätzlich ist ein definierter Prozess für regelmäßige Sichtungen und Überarbeitungen von Richtlinien notwendig. Dazu sollte in jeder Richtlinie dreierlei festgelegt werden:

- ein Intervall für eine regelmäßige Überprüfung der Angemessenheit und ggf. Aktualisierung der Richtlinie,
- das für die Überprüfung der Richtlinie verantwortliche Gremium oder die Rolle/Funktion, der diese Aufgabe zukommt, und
- die Angabe der Fundstelle, in der die jeweils aktuelle und gültige Fassung der Richtlinie verfügbar ist – z. B. eine Intranet-Adresse, die sich nicht ändert, wie die Startseite des Security-Intranets oder die Übersichtsseite aller gültigen Richtlinien des Unternehmens.

2.9 Ausnahmeregelung

Nur wenige Regelungen gelten ohne jede Ausnahme. Allerdings lassen sich zulässige Ausnahmen von einer Regel vorab selten vollständig auflisten. Daher hat es sich bewährt, Prozesse für die Zulassung von Ausnahmen und Abweichungen von einer Regelung festzulegen.

Wesentlich für solche Ausnahmeregelungen sind eine Verfahrensbeschreibung mit klaren Zuständigkeiten (Entscheidung über die Zulässigkeit einer Ausnahme), die Dokumentation der Ausnahmeregelung und eine zeitliche Befristung der Ausnahmegenehmigung. Diese ist durch Wiedervorlage nach Ablauf der Befristung zu prüfen und kann dann ggf. erneut befristet verlängert werden.

2.10 Anhänge

Im Anhang einer Richtlinie sollten sich Verweise auf alle wichtigen Dokumente finden, die in direktem Zusammenhang mit der Richtlinie stehen („Mitgeltende Dokumente"), wie z. B. die übergeordnete Security Policy oder das Unternehmensleitbild, Betriebsvereinbarungen oder konkrete Verfahrens- und Handlungsanweisungen.

Sofern die Richtlinie Prozesse regelt (wie z. B. eine Passwortrücksetzung), sollte sich im Anhang eine anschauliche Prozessbeschreibung beispielsweise in Gestalt eines Ablaufdiagramms finden. Auch Checklisten sind hilfreich, beispielsweise für die regelmäßige Überprüfung der Richtlinie (Was ist zu klären? Wer muss gefragt werden? Mit wem sind Änderungen abzustimmen?) oder die Inkraftsetzung und Bekanntgabe einer geänderten Richtlinie.

Auch ein Formblatt zur Dokumentation von Ausnahmegenehmigungen hilft, damit solche Fälle geeignet und vollständig dokumentiert werden.

Schließlich darf eine Liste der Ansprechpartner inklusive gültiger Kontaktdaten für eventuelle Rückfragen nicht fehlen.

Anhänge eignen sich auch zur Dokumentation vertraulicher Details einer Regelung, die nur einem begrenzten Empfängerkreis bekannt gemacht werden sollen. Außerdem sollten in Anhängen generell alle Aspekte geregelt werden, bei denen zu erwarten ist, dass sie vor Ablauf des Gültigkeits- oder des nächsten Überarbeitungszeitpunkts geändert werden müssen

und keine erneute Freigabe erfordern (z. B. Kontaktdaten oder Namen von Ansprechpartnern). Der Prozess zur Anpassung von Anhängen sollte jedoch einheitlich und klar geregelt sein.

3 Formale Aspekte

3.1 Dateiformat

Die Richtlinie sollte in einem Dateiformat veröffentlicht werden, das eine nicht-autorisierte Änderung des Dokuments möglichst ausschließt, beispielsweise als PDF-Datei, keineswegs in einem offenen Dokumentenformat.

Der Dateiname sollte „sprechend" gewählt werden und einen schnellen Rückschluss sowohl auf den Inhalt der Richtlinie (z. B. durch Verwendung eines gekürzten Titels) als auch auf die Dokumentenversion zulassen (z. B. durch eine Dateifolge- oder Versionsnummer). Dabei kommt es vor allem darauf an zu verhindern, dass unterschiedliche Versionen einer Richtlinie mit demselben Dateinamen kursieren.

3.2 Attribute

Weiter empfiehlt es sich, zu Beginn oder am Schluss einer Richtlinie wichtige Attribute in einem „Dokumentenprofil" zusammenzufassen, sofern sie nicht an anderer Stelle des Dokuments verwendet werden (bspw. in der Kopf- oder Fußzeile). Zu diesen Attributen können gehören:

- Dokumenten-ID
- (Richtlinien-)Titel
- Kurztitel
- Zusammenfassung
- Vertraulichkeitseinstufung
- Erstellungsdatum
- Umfang (Seitenzahl)
- (Bearbeitungs-)Status
- Version
- Erstellungsdatum + Ersteller
- Prüfungsdatum + Prüfer
- Freigabedatum + Freigeber (mit Rollenbezeichnung)
- Datum des Inkrafttretens
- Datum des Außerkrafttretens
- Datum der nächsten Prüfung
- Ablageort
- Anlagen
- Mitgeltende Regelungen
- Abgelöste Regelungen
- Verantwortung für die Vermittlung der Inhalte
- Sprachen (inkl. führende Sprache)

Die Erstellung eines solchen „Profils" kann durch einheitliche Dokumentvorlagen und eine automatisierte Formularabfrage zu Bearbeitungsbeginn vereinfacht werden.

Schließlich sollte das Dokument eine Änderungshistorie umfassen, aus der die wichtigsten inhaltlichen Änderungen (z. B. „Anpassung an CIO-Beschluss zur Mindestpasswortlänge") sowie Datum und Autor jeder Überarbeitung hervorgehen. Dabei ist nach jeder Änderung die Versionsnummer des Dokuments anzupassen.

3.3 Veröffentlichung

Die Lektüre von Richtlinien gehört sicherlich nicht zu den favorisierten Tätigkeiten von Mitarbeitern in Unternehmen. Dennoch ist es natürlich eine wesentliche Voraussetzung, dass Mitarbeiter Regelungsinhalte kennen, damit sie sie befolgen können. Dazu müssen sie insbesondere immer Zugriff auf eine aktuelle Version der sie betreffenden Richtlinien haben.

Es kann hilfreich sein, in Richtlinien einen Vermerk anzubringen, dass es sich bei einem Papierausdruck möglicherweise nicht um die aktuelle Version handelt – und vor der Lektüre der Richtlinie anhand der elektronischen Referenzfassung dessen Aktualität geprüft werden soll.

Schließlich kann ein einheitliches und ansprechendes Layout erheblich zur Verbesserung der Akzeptanz von Richtlinien in einer Organisation beitragen.