ISSN 1861-0641

IT-Sicherheit & Datenschutz

Ausgabe 03/06
17. 03. – 21. 04. 2006

Zeitschrift für rechts- und prüfungssicheres Datenmanagement

Praxis – Anwendungen – Lösungen

Sicherheits- und Datenschutz-Management

Grundlagen – Technik und Methoden

Vorschriften – Gesetze – Urteile

Online-Service
www.it-sd.com

VOGEL

Der Informationsdienst für IT-Manager,
IT-Sicherheits- und Datenschutzverantwortliche.

Professor Dr. Stephen D. Wolthusen

Risikomanagement, Sicherheitspolitiken und technische Verfahren zu deren Durchsetzung (I)

Das betriebliche Risikomanagement hat in den vergangenen Jahren aufgrund gesetzlicher Vorgaben auf nationaler und internationaler Ebene (z. B. KonTraG, Sarbanes-Oxley Act) sowie durch weitere indirekte regulierende Faktoren wie die Basel-II-Kreditvergaberichtlinien und allgemeine betriebliche Sorgfaltspflichten an Bedeutung gewonnen. Die daraus abgeleitete Sicherheitspolitik eines Unternehmens und die zugehörigen technischen Maßnahmen sind meist jedoch nur unter Schwierigkeiten umzusetzen.

Die Einführung einer betreiblichen Sicherheitspolitik und von Verfahren zu deren Umsetzung stellt Unternehmen vor große Herausforderungen

Aus den bei Einführung einer solchen Politik erforderlichen Risikoanalysen und -bewertungen ergeben sich in mehreren Verfeinerungsschritten Anforderungen an organisatorische und technische Abläufe. Diese wiederum bilden die unmittelbare Grundlage für die Erstellung der Sicherheitspolitik oder einer Menge von Sicherheitspolitiken, die aufeinander aufbauen. Erst davon ausgehend lassen sich technische Umsetzungsmaßnahmen zur Durchsetzung dieser Politik definieren und verfolgen.

Anforderungen an eine Sicherheitspolitik

Diese entstehen erstens dadurch, dass die Richtlinien auch für technische Laien verständlich sein müssen

Die wesentliche Herausforderung bei der Formulierung einer solchen Politik besteht somit darin, eine angemessene Balance zu finden: Das fertige Dokument soll hinreichend abstrakt die Probleme und daraus resultierenden Vorgehensweisen zur Sicherung der Werte der Organisation darstellen, muss aber konkret genug gefasst sein, um eine Abbildung der Sicherheitspolitik auf die technischen Maßnahmen zu ihrer Durchsetzung zu gewährleisten. Im engeren Sinn ist die Sicherheitspolitik also ein Dokument, das nicht technisch orientierte Entscheidungsträger vollständig unterstützen und deswegen insbesondere auch vollständig verstehen müssen. Umfang und Detaillierungsgrad sind also von vornherein notwendig beschränkt.

Zweitens darf ein solches Konzept nicht zu detailliert sein, da es sonst die flexible Reaktion auf Bedrohungen eher erschwert

Zudem erfordern Lebenszyklus und Zweck eines derartigen Dokumentes weitere Einschränkungen: Zum einen vergeht vom Entwurf einer Sicherheitspolitik und ihres Umsetzungskonzepts bis zur Zustimmung aller zu beteiligenden Entscheidungsträger geraume Zeit, in der detaillierte Festlegungen oft veralten. Zum anderen soll

die Sicherheitspolitik eine Organisation in die Lage versetzen, schnell und flexibel auf neue Bedrohungen zu reagieren, was allzu konkrete Vorgaben eher erschweren.

Bei der Formulierung der entsprechenden Weisungen und ihrer Umsetzung ist daher ein pragmatischer Ansatz zu wählen

Eine Sicherheitspolitik ist dabei der äußeren Form nach eine Weisung der Geschäftsführung; entsprechend muss für Mitarbeiter klar ersichtlich sein, dass die Geschäftsführung der IT-Sicherheit einen hohen Stellenwert beimisst. Dies ergibt sich außer aus den genannten inhaltlichen Gründen auch aus rechtlichen Anforderungen wie etwa datenschutzrechtlichen Belangen und Sorgfaltspflichten. Dabei sollten Unternehmen jedoch einen pragmatischen Ansatz verfolgen, denn eine zu ambitionierte Politik, die nicht oder nur sehr selektiv durchgesetzt wird, wirkt eher kontraproduktiv ist und zieht etwa durch unterschiedliche Sanktionsmaßnahmen bei Verstößen schnell den Vorwurf der Willkür auf sich.

Durchsetzung von Sicherheitspolitiken

Als besonders komplex und fehlerträchtig erweist sich zudem meist die Übersetzung der allgemeinen Vorgaben in technische Ziele

Die Umsetzung einer allgemeinen Sicherheitspolitik oder Familie von Sicherheitspolitiken, welche auf verschiedenen Organisationsebenen Regeln zur Einhaltung gesetzlicher oder anderweitig bindender Vorgaben einführen, erfordert eine Reihe von Übersetzungsschritten, die schließlich in konkrete technische Zielsetzungen münden. Dieser Vorgang sowie die anschließende Umsetzung z. B. mittels Neukonfiguration des Betriebssystems oder aktiver und passiver Netzwerkkomponenten umfasst ebenso wie die Ableitung der technischen Zielvorgaben selbst eine Reihe von Wahlmöglichkeiten und Alternativen. Je nach gegebener Zielsetzung sind dabei immer verschiedene Parameter (z. B. initiale Kosten, Erweiterbarkeit, Wartungskosten) zu betrachten und geplante Maßnahmen entsprechend zu optimieren; daher kann selbst bei vergleichbarer Ausgangslage aufgrund unterschiedlicher Erfahrungen und Präferenzen der Verantwortlichen das Resultat erheblich variieren. Problematisch sind hierbei vor allem die diesem Prozess inhärenten potenziellen Inkonsistenzen, die insbesondere in komplexeren Umgebungen mit heterogenen, verteilten Systemen auftreten. Diese ergeben sich etwa aus der Verwendung unterschiedlicher Betriebssysteme oder Betriebssystemversionen und Netzwerkkomponenten, die unterschiedliche Leistungsmerkmale aufweisen, oder durch Verzögerungen bei der Umsetzung in unterschiedlichen Teilbereichen eines Netzes.

Alle Schritte der vorgenannten Prozesskette beinhalten das Potenzial von Fehlern, gleich ob durch Missverständnisse, Unachtsamkeit oder Nachlässigkeit verursacht; bei der Umsetzung in konkrete technische Maßnahmen ist dies jedoch besonders ausgeprägt, da hier das Volumen der vorzunehmenden Schritte im Vergleich zu den abzuarbeitenden Abstraktionsebenen am größten ist. Es ist daher in hohem Maß wünschenswert, diese Prozesskette einheitlich, nachvollziehbar, und wo immer möglich automatisiert anzulegen, um Fehlerquellen weitestgehend zu beseitigen.

Grenzen von Standardsystemen

Ursache dafür ist vielfach der mangelnde Funktionsumfang verwendeter Standardsoftware

Ein gravierendes Problem, mit dem die technische Umsetzung der Sicherheitspolitiken konfrontiert ist, liegt im mangelnden Funktionsumfang der betroffenen Netzwerkkomponenten und Endgeräte. Vielfach sind die zur Verfügung stehenden Mechanismen, z. B. für die Zugriffskontrolle in Betriebssystemen, nicht mächtig und ausdrucksstark genug, um den Anforderungen einer abstrakten Sicherheitspolitik zu genügen. Dies führt oft dazu, dass in der Sicherheitspolitik als zwingend erachtete und angeordnete Maßnahmen und Kontrollen lediglich mit Hilfe organisatorischer Änderungen und Appellen an die Kooperationsbereitschaft der Nutzer durchgesetzt werden sollen. Da jedoch Mitarbeiter entsprechende Auflagen ihres Unternehmens in aller Regel nicht absichtsvoll verletzen, sondern zumeist Unkenntnis und Unachtsamkeit die unmittelbaren Ursachen sind, muss eine solche Strategie insgesamt unwirksam bleiben. Das gilt umso mehr, als selbst in Fällen, in denen Mitarbeiter solche Verstöße bewusst begehen, oft genug keine unlautere Absicht zugrunde liegt, sondern die Ursachen in der mangelnden Flexibilität der eingesetzten technischen Maßnahmen zu suchen sind, die ein offensichtlich legitimes Verhalten einschränken. Doch gerade bei der Verwendung von Standardsystemen lassen sich zumeist Wege finden, derartige Maßnahmen zu unterlaufen, so dass auch hier die Sicherheitspolitik aufgrund eines Mangels an technischen Möglichkeiten konterkariert wird.

Automatische Herleitung technischer Politikumsetzungsmaßnahmen

Das Fraunhofer-Institut für Graphische Datenverarbeitung (IGD) hat daher eine Lösung entwickelt, die eine automatische Herleitung erforderlicher technischer Maßnahmen ermöglicht

Einen Ansatz, den oben dargestellten Problemen zu begegnen, setzt das vom *Fraunhofer-Institut für Graphische Datenverarbeitung* (IGD) in Kooperation mit dem *Institute for Graphic Interfaces* (IGI) in Seoul seit 2002 betriebene Forschungs- und Entwicklungsprogramm COSEDA um. Ziel seiner Arbeit ist, durch die Integration von Ergänzungen in Standard-Betriebssysteme insbesondere der Windows-Familie, aber auch in Unix-Derivaten, einerseits die Möglichkeiten zur präzisen technischen Umsetzung von Sicherheitspolitiken zu verbessern und diese andererseits so einzubetten, dass bestehende Anwendungsprogramme und damit die Nutzer von diesen Veränderungen und Ergänzungen unberührt bleiben. Leitlinie ist dabei, die kognitive Belastung des Nutzers durch Einführung zusätzlicher Sicherheitsmechanismen so gering wie möglich zu halten. Wie dies konkret aussehen kann, zeigt Teil II dieses Beitrags im nächsten Heft.

Zum Autor:
Prof. Dr. Stephen D. Wolthusen ist Lecturer am *Department of Mathematics* der University of London und Associate Professor am *Norwegian Information Security Laboratory* in Gjövik.
E-Mail: Kontakt: stephen.wolthusen@rhul.ac.uk

BESTELLUNG

Per FAX an
0821 2177-35301

✗ Ja, ich möchte den Informationsdienst „IT-Sicherheit & Datenschutz“ abonnieren.

Sie erhalten im Jahrespaket „IT-Sicherheit & Datenschutz“ für insgesamt nur € 199,–
inkl. Versand, zzgl. MwSt.

- ✓ **12 Ausgaben „IT-Sicherheit & Datenschutz“**
- ✓ **52 eMail-Newsletter „Update“**
- ✓ **Ad-Hoc-News und Online-Konferenzen bei akuten Bedrohungen**
- ✓ **Online-Portal mit Vollzugriff auf den Premium-Bereich**

Bitte vollständig ausfüllen!

Firma

Name

Vorname

Funktion/Position

Straße/Nr.

PLZ/Ort

Telefon/Fax

E-Mail
(Meine Adresse und E-Mail-Adresse werden nicht an Dritte weitergegeben, es sei denn ich erteile dem Verlag dazu die Zustimmung. Der Verwendung meiner E-Mail-Adresse zum Zwecke der Übermittlung von Newsletter und Informationen zum Produkt „IT-Sicherheit und Datenschutz“ kann ich jederzeit widersprechen. Hierfür fallen keine anderen als die Übermittlungskosten nach den jeweiligen Basistarifen an.)

Dass ich damit einverstanden bin bestätige ich durch meine 2. Unterschrift.

Dieser Auftrag kann schriftlich innerhalb von 14 Tagen nach Absendung dieser Bestellung bei Vogel IT-Medien GmbH, Abo-Service IT-SD, Gutermannstraße 25, 86154 Augsburg widerrufen werden. Zur Fristwahrung genügt die rechtzeitige Absendung des Widerrufes in Form von Brief, Fax oder E-Mail. Die Kenntnisnahme des Widerrufsrechts bestätige ich durch meine Unterschrift.

Wenn ich mein Abo nicht mehr weiterbeziehen möchte, reicht bis sechs Wochen vor Ablauf des Bezugszeitraumes eine kurze schriftliche Nachricht an DataM-Services GmbH, Abo-Service IT-SD, 97103 Würzburg. Ansonsten verlängert sich der Bezugszeitraum jeweils um ein weiteres Jahr. Es gelten dann die regulären Preise der jeweils aktuellen Preisliste.

✗ Datum, Unterschrift

✗ 2. Unterschrift

Vogel IT-Medien, Gutermannstr. 25, 86154 Augsburg, Tel. 0821 2177-0, www.vogel-it.de, Geschäftsführer: Werner Nieberle, HRB 11943

Per Telefon: 0821 2177-301
Per Fax: 0821 2177-35301
Per E-Mail: vertrieb@it-sd.com
Im Internet: www.it-sd.com