HELPDESK

Mit System zur IT-Sicherheitsrichtlinie

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.

ILLUSTRATION: CW/THÜ

Frage: Was beinhaltet eine Sicherheitsrichtlinie und wie kann sie mit möglichst wenig Aufwand erstellt werden?

Die Problemstellung ist klassisch: Einerseits hat die Geschäftsleitung eine aus der Unternehmensstrategie abgeleitete langfristige Security-Strategie in Form eines halb- bis mehrseitigen Dokuments abgesegnet. Andererseits wurden daraufhin im Zuge der organisatorischen Umsetzung als Sofortmassnahme Security Policies, Weisungen und Checklisten verfasst und in Kraft gesetzt. Aber der Mittelbau, die Verbindung der strategischen mit der operativen Ebene, fehlt oftmals. Diese Lücke schliesst die so genannte IT-Sicherheitsrichtlinie, ein Dokument, welches über hundert A4-Seiten umfassen kann, dafür aber sämtliche, für ein effektives und effizientes IT-Security-Management benötigten Bereiche abdeckt.

Das Verfassen einer IT-Sicherheitsrichtlinie mittels Konsolidierung bestehender sicherheitsrelevanter Dokumente bietet die Chance, das Informationssicherheitsmanagement nachhaltig zu verbessern, indem Widersprüche beseitigt und so genannte «weisse Flecken» auf- und anschliessend abgedeckt werden. Security Policies werden üblicherweise bezüglich Inhalt und Formulierung auf die Zielgruppe ausgerichtet. Wenn keine zentrale Koordination der Dokumente erfolgte, ist die Wahrscheinlichkeit gross, dass die Policies sich zumindest bezüglich der verwendeten Formulierungen unterscheiden. Schwerer wiegen andere potenzielle Probleme – etwa, dass nicht alle Bereiche abgedeckt wurden oder sich einzelne Weisungen und Regelungen widersprechen. Widersprüche mittels eines Direktvergleichs der einzelnen Dokumente untereinander aufzudecken ist reine Fleissarbeit. Anders verhält es sich mit allfällig bestehenden weissen Flecken.

> «Standards können als Checklisten dienen, um sicher zu stellen, dass keine wichtigen Aspekte vergessen werden.»

Standards

Hier kommen Standards ins Spiel. Sie können unter anderem als Checklisten dienen, um sicher zu stellen, dass keine wichtigen Aspekte vernachlässigt werden. Ein vielfach bewährter Standard ist ISO/IEC 17799, auch als «Code of practice for information security management» bekannt. Die im Juni 2005 publizierte Neuauflage ISO/IEC 17799:2005 wird voraussichtlich nach abgeschlossener Vernehmlassung durch die nationalen Normenausschüsse per 2007 zur neuen Norm ISO/IEC 27002 erklärt. Somit ist jeder gut beraten, sich bereits mit der aktuellen Version von 17799 zu beschäftigen. Sämtliche ISO-Normen können gegen Entgelt bei der Schweizerischen Normen-Vereinigung SNV (www.snv.ch) bezogen werden.

Methode

Folgende Methode beschreibt einen pragmatischen Bottom-up-Ansatz, welcher auf bestehendem aufbaut, um den Erstellungs- und den anschliessenden Kommunikationsaufwand zu minimieren. Sämtliche vorhandenen sicherheitsrelevanten Dokumente wie beispielsweise Security-Strategie, Policies und allfällige Anhänge des Arbeitsvertrags betreffend Umgang mit Informatikmitteln und das Inhaltsverzeichnis der Norm 17799 werden ausgedruckt. Anschliessend werden die Titel und Untertitel des Inhaltsverzeichnisses der Norm ausgeschnitten und ausgelegt. Nun werden die sicherheitsrelevanten Dokumente gelesen, Themen abschnittsweise ausgeschnitten und den Kapiteln und Unterkapiteln zugeordnet. Nachdem alle Dokumentspassagen ausgelegt wurden, sind Widersprüche leicht erkennbar. Weisse Flecken erkennt man daran, wenn keine Dokumentenabschnitte den Titeln/Untertiteln zugeordnet werden konnten.

Nun gilt es bestehende Passagen anzupassen und fehlende zu ergänzen. Die Erfahrung zeigt, dass der vom bestehenden Dokumentationsgrad abhängige Aufwand für die Erstellung einer IT-Sicherheitsrichtlinie bei zirka 10 bis 20 Personentagen liegt – aus Sicherheitssicht eine lohnenswerte und nachhaltige Investition. ■

Der Autor
Christoph Baumgartner ist Consultant und OPST bei der Sicherheitsberaterin Oneconsult, Thalwil, www.oneconsult.com.

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch