Computerworld 7/8. Mai 2015
→ www.computerworld.ch

FOKUS: SECURITY

Rezepte, mit denen nichts anbrennt

Standards in der IT-Sicherheit stützen sich auf bewährte Strategien und sorgen dafür, dass nichts vergessen geht. Ein Überblick über die gebräuchlichsten Standards und ihre Anwendungsgebiete. → VON CATHRIN SENN

Vielfältige Bedrohungen der IT-Sicherheit machen das Thema nicht nur in den Medien präsent, sondern sorgen vermehrt auch für Gesprächsstoff in den Geschäftsleitungen von Unternehmen. Diese «Management Attention» erzeugt oft den Wunsch, einen Überblick über die IT-Sicherheit in der eigenen Organisation zu gewinnen und diese messbar zu machen. An diesem Punkt setzen IT-Sicherheits-Standards an.

WARUM IT-SICHERHEITS-STANDARDS?

Das Ziel der IT-Sicherheit ist es, Hard- und Software, physische Einrichtungen und vertrauliche Daten zu schützen, um damit finanzielle Verluste, Personen- und Imageschäden zu vermeiden sowie gesetzliche und andere Anforderungen einzuhalten. Den Standards kommt dabei eine bedeutende Rolle zu, einerseits, weil sie auf anerkannten Ansätzen und Best Practices aufbauen, andererseits, weil manche Standards die Möglichkeit einer Zertifizierung bieten.

WORIN SIE SICH UNTERSCHEIDEN

Für die IT-Sicherheit gibt es eine ganze Reihe von Standards. Bei Frameworks wie COBIT und ITIL oder bei der Norm ISO/IEC 20000 wird die IT als Ganzes aus der Governance- respektive Operations-Perspektive betrachtet. Die Sicherheit fliesst dabei als Thema mit ein. Bei anderen Standards hingegen ist IT-Sicherheit das alleinige Thema.

Die Standards unterscheiden sich vor allem darin, auf welcher Flughöhe sie sich mit Sicherheit beschäftigen. Während ISO/IEC 27001 und 27002 die Informationssicherheit als Ganzes betrachten – also neben der IT-Security auch noch weitere Aspekte wie die physische Sicherheit abdecken –, konzentrieren sich Standards wie ISO/IEC 27033 (Network Security) auf bestimmte Gebiete der IT-Sicherheit.

Weiter können IT-Security-Standards danach eingeteilt werden, ob sie branchenspezifisch sind oder für alle Arten von Organisationen gelten, ob sie kostenpflichtig sind und ob eine Zertifizierung möglich ist. In der Tabelle oben rechts auf dieser Doppelseite sind exemplarisch einige wichtige Standards aufgeführt und nach ihrer Ausrichtung kategorisiert.

INFORMATION SECURITY FRAMEWORKS

Eines der bekanntesten Information Security Frameworks besteht aus der ISO/IEC-2700X-Familie. Der einzige Standard dieser Gruppe, nach dem man sich zertifizieren lassen kann, ist ISO/IEC 27001. Er beschreibt die Anforderungen an ein Information Security Management System (ISMS) und ist mit anderen ISO-Managementsystemen wie ISO 9001 (Qualitätsmanagement) vergleichbar. Annex A dieses Standards führt Informations-Sicherheits-Massnahmen auf, die in der Norm 27002 weiter ausgeführt werden.

«Die Critical Security Controls liefern einen kompakten Ansatz zur Verbesserung der IT-Sicherheit»

Cathrin Senn

Der deutsche IT-Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik (BSI) orientiert sich an ISO/IEC 27001 und 27002. Eine Zertifizierung ist möglich. Sie umfasst sowohl die Zertifizierung nach ISO/IEC 27001 als auch die Prüfung der Sicherheitsmassnahmen auf der Basis von IT-Grundschutz und geht deshalb tiefer. Allerdings sind die IT-Grundschutz-Standards, die aus dem Jahr 2008 stammen, noch nicht an die neuste Version ISO/IEC 27001:2013 angeglichen.

BILD: ISTOCKPHOTO.COM/KZENON

Wichtige IT-Sicherheits-Standards

Standard	Beschreibung	kostet	Zertifizierung
ISO/IEC 27001	Beschreibt die Anforderungen an ein Information Security Management System (ISMS)	ja	ja
ISO/IEC 27002	Leitfaden für die Implementierung von Information-Security-Massnahmen basierend auf ISO/IEC 27001 Annex A	ja	nein
IT-Grundschutz	Umfasst die BSI-Standards 100-1 bis 100-4 und die IT-Grundschutz-Kataloge; ist kompatibel mit ISO/IEC 27001	nein	ja (ISO/IEC-27001-Zertifizierung auf der Basis von IT-Grundschutz)
NIST SP 800-X	Eine Serie von Guidelines und Empfehlungen des US-amerikanischen National Institute of Standards and Technology	nein	nein

Die Standards unterscheiden sich unter anderem im Grad der Spezialisierung

IT-SECURITY-STANDARDS

Die Serie Special Publications 800 des US-amerikanischen National Institute of Standards and Technology enthält primär IT-Security-Standards. Die Sammlung umfasst Einführungen und Guidelines zu vielen verschiedenen Themen wie Sicherheit von WLANs, Cloud Computing, Mobile Devices und IPv6. Eine spezielle Publikation ist SP 800-53, die für US-Bundesbehörden gilt und einen Katalog von Information Security Controls beinhaltet, die auch auf die Massnahmen von ISO/IEC 27001:2013 Annex A gemappt sind. Eine Untermenge der Controls aus SP 800-53 stellen die «Critical Security Controls» dar, die vom Council on Cyber-Security herausgegeben werden (vorher SANS Institute) und 20 Massnahmen für die am weitesten verbreiteten Angriffe beschreiben.

BRANCHENSPEZIFISCHE STANDARDS

Die 27000er-Reihe enthält einige Standards, die branchenspezifische Eigenheiten der Sicherheit berücksichtigen. So bildet zum Beispiel ISO/IEC TR 27015 eine Leitlinie für Finanzdienstleister und ist als Ergänzung zu ISO/IEC 27002 gedacht, der alle Arten von Organisationen abdeckt und damit sehr generisch ist. Analog dazu existieren Richtlinien für das Gesundheitswesen, den Energiesektor und die Telekommunikation.

Für industrielle Steuerungssysteme (Stichwort ICS oder SCADA), die wiederum spezielle Anforderungen an die Sicherheit stellen, sind spezifische Standards entwickelt worden. Dazu gehören der internationale IEC 62443 für Industrie-Kommunikationsnetzwerke, die US-amerikanischen NERC CIP Standards (CIP = Critical Infrastructure Protection) oder der deutsche VDI/VDE 2182 für die Informationssicherheit in der industriellen Automatisierung.

Der bekannte PCI DSS (Payment Card Industry Data Security Standard), ein eigener Datensicherheits-Standard der Zahlungskartenbranche, betrifft alle Unternehmen, die Zahlungen mit Kreditkarten wie Visa, MasterCard, American Express etc. abwickeln. Das Regelwerk soll Kreditkartenbetrug verhindern, indem Massnahmen zur Sicherheit von Karteninhaberdaten ergriffen werden. Ein wichtiges Einsatzgebiet sind E-Commerce-Anbieter, die Zahlungen mit Kreditkarte akzeptieren (online oder aber auch telefonisch). Je nach Anzahl Transaktionen pro Jahr mit einer spezifischen Karte müssen bestimmte Sicherheitsanforderungen erfüllt werden.

EMPFEHLUNGEN AUS DER PRAXIS

PCI DSS ist für Unternehmen, die Kreditkartenzahlungen abwickeln, verpflichtend. Andere Standards wie ISO/IEC 27001 bieten die Möglichkeit, sich freiwillig zertifizieren zu lassen, sodass man sich die Konformität mit der entsprechenden Norm bestätigen lassen und dem Management oder den Kunden kommunizieren kann.

Während ISO/IEC 27001 auf das Management eines Informationssicherheitssystems fokussiert und relativ viel Spielraum bei der Interpretation offen lässt, bieten ISO/IEC 27002 und der IT-Grundschutz konkrete Hilfestellung bei der Implementierung von Informationssicherheitsmassnahmen. Sie können massgeblich zu einer Erhöhung der Informationssicherheit beitragen, wenn keine Zertifizierung angestrebt wird. Das kann durchaus der Fall sein, denn eine Zertifizierung ist relativ aufwendig und deshalb nur für einen eingeschränkten Geltungsbereich sinnvoll (z. B. ein bestimmtes System, eine Abteilung, ein Standort oder eine Kombination davon).

Die in den Standards aufgeführten Massnahmen müssen nicht alle zutreffen (wenn z. B. intern keine Software entwickelt wird). Sie decken aber wichtige Punkte ab, die helfen, die IT- und Informations-Sicherheit technisch, organisatorisch und im Hinblick auf Prozesse und die Dokumentation zu verbessern. Unterstützend dazu können auch die entsprechenden branchenspezifischen Standards der ISO/IEC-27000er-Reihe zurate gezogen werden.

Einen kompakten Ansatz zur Verbesserung der IT-Security bieten die «Critical Security Controls». Während Standards wie ISO/IEC 27001 und ISO/IEC 27002 relativ umfassend sind, fokussieren die 20 Controls auf verbreitete Angriffe und enthalten die sogenannten «First Five Quick Wins», die als Erstes angegangen werden können.

Um einen Gesamtüberblick über die Informations- resp. IT-Sicherheit zu gewinnen, empfiehlt sich ein Audit mittels Fragebogen oder Interview. Das Audit führt eine interne oder externe Stelle anhand eines Standards wie ISO/IEC 27002 durch. Es kann aufzeigen, wo Sicherheitslücken vorhanden sind und die Security Awareness durch die Durchführung des Audits bei Mitarbeitenden und Management steigern.

FAZIT: HILFREICHE STÜTZEN

Standards werden vom Management meistens anerkannt und sparen Zeit, da sie sich auf bestehende Best Practices stützen. Sie verhindern zudem, dass wichtige Punkte vergessen gehen. Zwar sind sie kein Sicherheitsallheilmittel, aber eine sinnvolle Stütze, um Organisationen bei der Umsetzung der IT-Security zu begleiten. ←

Dr. Cathrin Senn ist ISO 27001 Lead Auditor, CCO & Partner bei Oneconsult → **www.oneconsult.com**