SPEZIAL

itsecurity

Sonderdruck für:

HiScout

Standardisiertes Vorgehen mit BSI IT-Grundschutz

Grundschutz von der Stange?

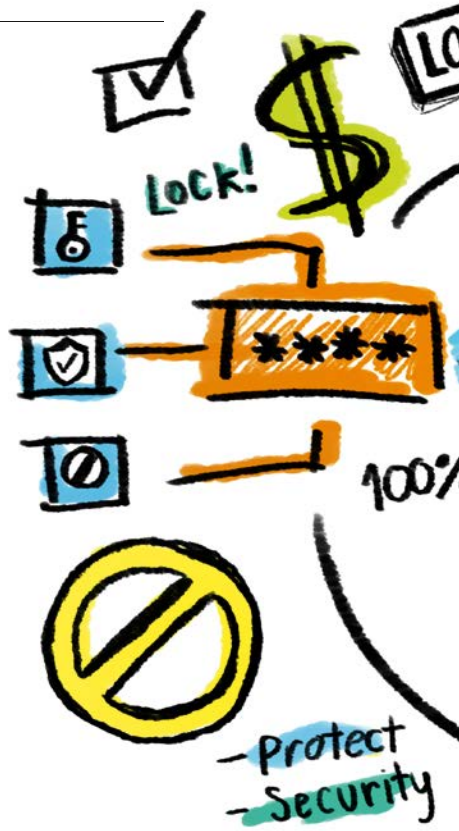
Internet of Things

Euphorie vs. Risiken

Thomas Gross, Clavister, über die Gefahren des Internet of Things

Standardisiertes Vorgehen mit BSI IT-Grundschutz

Grundschutz von der Stange?



Auch ein vermeintlich bis ins Detail spezifizierter Standard wie die BSI Grundschutz-Vorgehensweise bietet viel Raum für Individualisten. Warum Anpassungen des Vorgehens oft sinnvoll sind, Entscheidungen selten ewig gelten und wie dies in der Toolauswahl berücksichtigt werden kann, lesen Sie hier.

Kaum ein Unternehmen stellt heutzutage noch die Notwendigkeit des Betriebs eines ISMS in Frage und meidet die nötigen Investitionen. Bedenkt man wie schwer es ist, diesen Aufwänden einen Ertrag entgegenzusetzen, sind diese Investitionen in die Zukunft ein gutes Zeichen bezüglich des geschärften Bewusstseins für die wachsende Bedrohungslage, welcher sich sowohl die öffentliche Hand, als auch die freie Wirtschaft stellen müssen.

Entgegen der grundsätzlichen Entscheidung zur Freigabe der Ressourcen, ist die Frage nach dem genutzten Standard für das IT-Sicherheitsmanagementsystems schwieriger zu beantworten. Gesetzt den Fall, dass die Organisation nicht bereits durch gesetzliche Vorgaben zur Nutzung des IT-Grundschutzes angehalten wird, gilt es zu evaluieren welche Anforderungen das Unternehmen selbst, sowie die weiteren interessierten Parteien (zum Beispiel Geschäftspartner) an das Unternehmen stellen.

WEB-TIPP:
www.hiscout.com

Bei der Wahl des Standards ist zu berücksichtigen, dass der Detailgrad, in welchem die IT Grundschutz-Vorgehensweise definiert ist, nicht als Einschränkung, sondern als kostenfreie, vielfach bewährte Hilfestellung begriffen werden sollte. Hier hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) über die Jahre einen nicht zu unterschätzenden Beitrag für das Sicherheitsniveau im gesamten deutschsprachigen Raum geleistet. Die Kombination aus klarem Vorgehen, gepaart mit den Grundschutzkatalogen, ist ein immenser Gewinn für jeden der sich mit dem Thema beschäftigt. Eine große Menge an Fachwissen steht direkt zur Verfügung und muss nicht aufwendig über das Risikomanagement, Audits und Sicherheitsvorfälle erkannt werden. Setzt man daher die Erhöhung des Sicherheitsniveaus in Relation zur Dauer der Einführung, dürfte dem BSI IT-Grundschutz kein weiterer Standard gewachsen sein.

Standard versus Individualismus?

Natürlich dient ein Standard u.a. dazu Eckpunkte festzulegen, eine Vergleichbarkeit zu ermöglichen und dafür Sorge zu tragen, dass ein Vorgehen so implementiert wird, wie es der Herausgeber vorsieht. Daraus zu folgern, dass der IT-Grundschutz-Standard wenig Raum für die optimale Ausrichtung an der individuellen Wirklichkeit des Unternehmens zulässt, wäre jedoch falsch.

> „Die Abbildung von individuellen und sich stetig entwickelnden Sicherheitsprozessen erfordert eine hohe Flexibilität auf der Toolseite."
>
> Tobias Seemann,
> HiScout GmbH

Bereits bei der Strukturanalyse und der Schutzbedarfsfeststellung gilt es den Aufwand sowohl auf Seite der IT, als auch auf Seite des Sicherheitsbeauftragten möglichst gering zu halten. Die Strukturanalyse in einer Form durchzuführen, welche massiv von der Datenstruktur der IT abweicht, führt schnell zu unnötig hohen Aufwänden. Sowohl bei der initialen Aufnahme, als auch bei der Pflege wird die Datenqualität vermindert und führt zu Spannungen. Hat die IT etwa den Service-Gedanken verinnerlicht, bietet den Fachprozessen IT-Services an und pflegt benötigte Ressourcen als Servicekomponenten, dann gilt es, das Grundschutz-Vorgehen im Unternehmen anzupassen. Dies schlägt sich anschließend auch in einer Vereinfachung der Schutzbedarfsfeststellung nieder. Der Schutzbedarf kann dann beispielsweise am Prozess erhoben und über die gebuchten Services vererbt werden, was im Gegenzug auch einen zusätzlichen Informationsgewinn für das Servicemanagement darstellt.

Neben diesem und vielen weiteren möglichen Beispielen für individuelle Anpassungen innerhalb des Standards 100-2, gilt es natürlich auch, das große Ganze nicht aus den Augen zu verlieren. Die Aufgabe der IT-Sicherheit ist bei weitem nicht mit der Dokumenta-

tion eines Sicherheitskonzeptes für einen oder mehrere Verbünde erfüllt. In jeder Organisation gibt es eine Vielzahl an Sicherheitsprozessen, welche gelebt werden müssen. Diese sind der „Fingerabdruck" der Organisation und in ihrer Ausprägung stets individuell.
Bewegt man sich in einem Managementsystem, so trifft der Grundgedanke eines Regelkreises zu. Dies bedeutet, dass stetige Überprüfung und Anpassung des Systems feste Bestandteile und bei einer möglichen Zertifizierung sogar verpflichtend sind. Die Ausgestaltung des Systems nimmt daher eine höchst individuelle Ausprägung an und befindet sich stetig im Wandel. Prozesse, welche sich heute noch mit einer Excel-Datei auf einem geschützten Netzlaufwerk managen lassen, können durch Compliance-Anforderungen oder den Zwang zur Effizienz schon morgen einen dokumentierten, verteilten und revisionssicheren Prozess erfordern.

Bedeutung für die Toolauswahl

Mit der Abkündigung des Supports für das GSTOOL, der Einführung des IT Sicherheitsgesetzes und der Modernisierung des Grundschutzes durch das BSI entsteht für die Toolhersteller ein spannender Markt mit viel Bewegung.

Die Pflicht, das IT-Grundschutz-Vorgehen gemäß BSI Standard 100-2 abzubilden, beherrschen aufgrund der klaren Vorgaben fast alle Anbieter eines „alternativen GSTOOL". In der Kür sind die Unterschiede jedoch groß.

Soll die Gelegenheit genutzt werden, die Toolunterstützung signifikant zu verbessern, so muss zunächst festgelegt werden, ob der komplette Betrieb eines Informationssicherheitssystems durch einen Tooleinsatz unterstützt werden soll. Die Frage nach dem grundsätzlichen Betrieb eines ISMS wird vielen Unternehmen dabei bereits durch entsprechende Paragraphen im IT-Sicherheitsgesetz abgenommen. Je nach Bedarf trennt sich bei den Toolherstellern die Spreu vom Weizen. Nur ein Teil der Anbieter unterstützt die Sicherheitsprozesse oder weitere Managementdisziplinen wie Business Continuity oder Compliance Management, welche sich beispielsweise in den Maßnahmen der übergreifenden Aspekte oder den weiteren BSI Standards finden.

Bezüglich der Prozessunterstützung ist auch darauf zu achten, was der Anbieter tatsächlich unter Workflows versteht. Zwischen einer „Prozessdokumentation", also der einfachen Mitschrift, dass eine bestimmte Aktion erledigt ist und einem tatsächlichen, rollenbasierten Userbereich mit anstehenden Aufgaben, sind auf dem Markt viele Variationen vorhanden.

Selbst unter Zeitdruck sollte es vermieden werden, sich auf eine eventuell ungeeignete oder eingeschränkte Lösung einzulassen. Vielmehr sollte auf ein Tool gesetzt werden, welches zwei zentrale Eigenschaften besitzt: Zum einen sollte es im Auslieferungszustand leicht bedienbar und exakt am BSI-Standard ausgerichtet sein, um den initialen Ein- oder Umstieg möglichst einfach zu gestalten. Zum anderen sollte es durch einfache Anpassbarkeit und eine flexible Plattform in der Lage sein, spätere Erweiterungen und Anpassungen problemlos zu unterstützen, damit der Grundschutz von der Stange zum Maßanzug werden kann.

Tobias Seemann

HiScout

HiScout GmbH
Bouchéstraße 12
12435 Berlin // Germany
Tel. +49 30 33 00 888-0
Fax +49 30 33 00 888-99
E-Mail: GRC-Suite@hiscout.com
Web: www.hiscout.com