SCHWERPUNKT IT-INFRASTRUKTUR FÜR SICHERHEITSTECHNIK

RICHTLINIE

Das BSI hilft

Um eine Vorgabe für Aufbau und IT-Betrieb von Sicherheitstechnik zu schaffen, ist die beliebte ISO27001/2 Norm zu „generisch". Die darin aufgeführten Controls haben gewiss Gültigkeit, helfen aber bei konkreten Fragestellungen nicht recht weiter. Erheblich ergiebiger ist hierzu ein Blick in das Grundschutzkompendium des Bundesamtes für Sicherheit in der Informationstechnik, BSI. Auch hier gibt es (noch) keine spezielle Behandlung der IT-gestützten Sicherheitstechnik, aber mit den Abhandlungen zu „IND.1 Betriebs- und Steuerungstechnik" kommt man den Problemen und Fragestellungen ganz nah.

OT = SIT

Im folgenden Abschnitt hat der **Sicherheits-Berater** nur das Kürzel „OT" (für Operational Technology") durch „SIT" (Sicherheitstechnik-IT) ersetzt, ansonsten entspricht der Text den Ausführungen des BSI zur industriellen IT:

Hoher Verfügbarkeitsbedarf

Die in der Vergangenheit übliche physische Trennung der SIT von anderen IT-Systemen und Netzen in Büroanwendungen ist heute aufgrund zunehmender Integrationsanforderungen nur in Ausnahmefällen bei erhöhtem Schutzbedarf anwendbar. Da neben SIT-spezifischen Komponenten zunehmend IT-Komponenten und Technologien aus der Office-IT in der SIT eingesetzt werden, sind diese inzwischen vergleichbaren Gefährdungen ausgesetzt. Zugleich weisen die SIT gegenüber der klassischen IT wesentliche Unterschiede auf, die das Anwenden dort etablierter Sicherheitsverfahren erschweren. So kann es Restriktionen aufgrund von Herstellervorgaben oder gesetzlichen Anforderungen geben, die Veränderungen an Komponenten verhindern oder erschweren. Ein Beispiel hierfür sind die Anwendung von Sicherheitsupdates oder nachträgliche Härtungsmaßnahmen. Ein wesentlicher Unterschied ergibt sich für die SIT auch aus den oft hohen Verfügbarkeits- und Integritätsanforderungen, während im Vergleich zur Office-IT die Vertraulichkeit häufig von nachrangiger Bedeutung ist. Störungen dieser Systeme können Gefährdungen von Leib, Leben und Umwelt nach sich ziehen und sind zumeist nicht durch einen Neustart zu beheben.

Passt.

» Ersetzen Sie OT durch SIT, dann passen die BSI-Ausführungen. «

Umsetzung der MUSS-Maßnahmen

Nun kann man für einen ersten Check einfach die Normensprache nutzen, die das BSI in den Bausteinen des Kompendiums benutzt. Das Minimum an Informationssicherheit, das für einen sicheren Einsatz von IT-gestützter Sicherheitstechnik vorzuweisen ist, ist die geeignete Umsetzung der Basisanforderungen, also der MUSS-Maßnahmen, die in einem solchen Baustein des Grundschutzkompendiums aufgeführt sind.

Maßnahmen:
Da es eine in 20 Jahren Praxis validierte Erkenntnis des Verfassers ist, dass auch ein derart deutlicher Verweis auf einen längeren Text des BSI nicht dazu führt, dass dieser Text anschließend gelesen wird, folgt die Aufstellung der auf das Thema SIT modifizierten BSI-Anforderungen:

Gesamtverantwortlicher

1. Es MUSS ein Gesamtverantwortlicher für die Informationssicherheit im SIT-Bereich bestimmt und innerhalb der Institution bekanntgegeben werden.

Compliance

2. Gesetzliche, regulatorische und sonstige besonderen Vorgaben für den SIT-Bereich sowie die jeweilige Branche bzw. den Sektor MÜSSEN bekannt und ihre Auswirkungen auf die Institution ausgewertet sein.

Aufbau einer Sicherheitsorganisation

3. Die Leitungsebene der Institution MUSS den Sicherheitsprozess initiieren, steuern und kontrollieren. Die Institution MUSS eine Sicherheitsorganisation aufbauen, welche die Rollen und Verantwortlichkeiten für die Informationssicherheit der SIT-Infrastruktur und -Komponenten regelt.

Umsetzung der Vorgaben

4. Es MUSS ein Prozess existieren, wie konkrete Vorgaben (Richtlinien) für bestimmte Themenbereiche im Prozessbereich verfasst, kommuniziert, zur Umsetzung gebracht, fortgeschrieben, bewertet und verbessert werden.

Sensibilisierung

5. Betriebspersonal MUSS regelmäßig zu relevanten IT-Sicherheitsbedrohungen im SIT-Bereich informiert und sensibilisiert werden. SIT-Verantwortliche MÜSSEN regelmäßig zur Bedrohungslage und Handlungsbedarfen informiert oder geschult werden.

Schutz vor Schadprogrammen

6. Zur Vorbeugung vor Risiken durch Schadprogramme MUSS ein Konzept zum Schutz vor Schadprogrammen erstellt und umgesetzt werden. Darin MÜSSEN die bedrohten IT-Systeme sowie die möglichen Infektionswege (Außenschnittstellen, Wechselmedien, Service- und Parametrier-/Programmiergeräte) betrachtet und geeignete technische und organisatorische Schutzmaßnahmen festgelegt sein.

Support bei Virenschutz

7. Beim Einsatz von Virenschutzsoftware auf SIT-Komponenten MUSS berücksichtigt werden, ob und in welcher Konfiguration der Betrieb von Virenschutzsoftware vom Hersteller unterstützt wird. Ist dies nicht der Fall, MUSS im Rahmen einer Risikoanalyse der Bedarf an alternativen Schutzverfahren geprüft werden.

8. Eingesetzte Virenschutzsoftware MUSS mit aktuellen Signaturen versorgt werden.

Aktualisierung

9. Das Virenschutzkonzept MUSS die Aktualisierungsstrategie festlegen. Dies umfasst den Bezug von Signaturen, deren Verteilungsverfahren und die Häufigkeit der Aktualisierung. Der Bezug und die Verteilung von Signaturen können automatisiert erfolgen.

Kein Internetdownload

10. Der Bezug von Virensignaturen durch SIT-Systeme DARF NICHT direkt aus dem Internet erfolgen, sondern MUSS indirekt über einen Proxy- oder Virensignaturverteildienst erfolgen.

11. Die Schnittstellensysteme MÜSSEN in einer eigenständigen Zone (z. B. DMZ) von der SIT-Umgebung getrennt betrieben werden.

Voraussetzungen geschaffen

Diese 11 Punkte sind für das oder die IT-Netze, in denen Videoüberwachung, Zutrittskontrolle und Gefahrenmeldeanlagen betrieben werden, recht einfach zu verifizieren. Erst wenn Verantwortung und Zuständigkeit geregelt sind und der Schutz vor Schadsoftware sowie die Abtrennung des Netzes von anderen Netzen sichergestellt sind, muss man sich Gedanken um mehr machen. Dokumentation und geregelter IT-Betrieb, die Benutzerverwaltung, Patch-, Change- und Incidentmanagement sind gewiss Themen, die vernünftig umgesetzt werden müssen. Voraussetzung dafür sind aber klare Zuständigkeiten und ein separates Netz. ::: Werner Metterhausen :::