VORSTUFE ZUM IT-GRUNDSCHUTZ RS7 – INFORMATIONSSICHERHEIT FÜR EINSTEIGER

Das Erstellen von Sicherheitskonzepten ist ein aufwendiger Prozess und erfordert neben technischem auch umfassendes methodisches Vorwissen über den IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik. RS7 („Recht Sicher in 7 Schritten“) bietet eine schlanke und effiziente Vorstufe zum Grundschutz, der bei Bedarf jedoch nahtlos auf RS7 aufgesetzt werden kann.

| von IRENA IRMLER

Unsere Gesellschaft ist in wachsendem Maße von Informationen abhängig. Wurden bestimmte Daten versehentlich oder absichtlich gelöscht, manipuliert oder offengelegt, so kann dies erhebliche Folgen für Individuen, Unternehmen und Behörden haben. Um sensible Informationen angemessen und umfänglich zu schützen, ist ein umfassender und systematischer Ansatz unabdingbar. Zu diesem Zweck hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den IT-Grundschutz entworfen, der auf die Absicherung von definierten Informationsverbünden zielt. Seine Anwendung ist für Bundesbehörden verpflichtend.

Wer gerade ein Sicherheitskonzept nach IT-Grundschutz erstellt oder zu erstellen plant, kennt das Problem: Das Erstellungsverfahren des BSI ist zwar solide und verlässlich, aber gleichzeitig langwierig und so komplex, dass in den meisten Fällen externe Unterstützung notwendig ist.

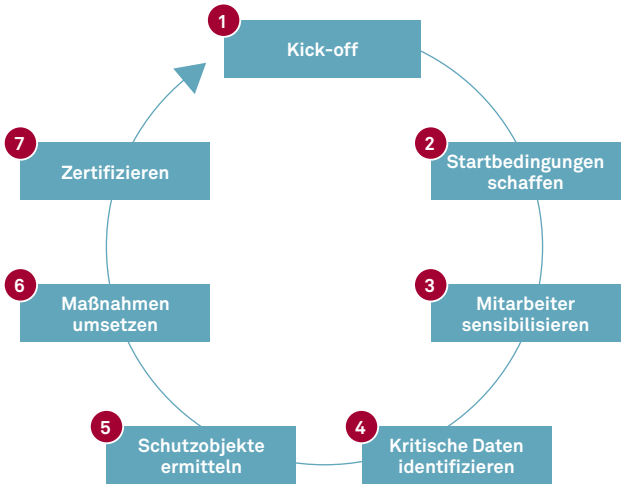

Abbildung 1: Der RS7-Zyklus

Dagegen ist RS7 ist ein schlankes, einfaches Informationssicherheits-Managementsystem (ISMS). Es richtet sich an alle, für die die Anwendung von IT-Grundschutz noch nicht erforderlich ist oder die sich dem Thema erst noch annähern müssen. Das sind zum Beispiel Kommunen, IT-Verfahren, Arbeitsbereiche, die laufende Geschäftsprozesse zügig absichern möchten, ohne den umfassenden und komplexen Ansatz des Grundschutzes durchexerzieren zu müssen. Mit in der Riege der potenziellen Anwender sind das auch größere Mittelständler, Verbände oder sonstige behördennahe Organisationen, die zwar nicht dem Grundschutz verpflichtet sind, aber schnelle Sicherheitsgewinne mit einem durchdachten Verfahren erzielen möchten.

RS7 bietet ein leicht verständliches Vorgehen in sieben Schritten mit Erläuterungen und Vorlagen für die Dokumentation (siehe Abbildung 1). Um die organisatorischen und technischen Bedingungen vor Ort so realitätsgetreu wie nötig und so abstrakt wie möglich abzubilden, ist das System modular aufgebaut. Auf dieser Basis können direkt Maßnahmen identifiziert und umgesetzt und zügig sowie ohne großen Aufwand eine spürbare Erhöhung der Informationssicherheit erzielt werden.

DER RS7-PROZESS

Der erste Schritt „Kick-off" stellt den Startschuss für den RS7-Prozess dar: In einem strukturierten Termin mit allen Anspruchsgruppen wird definiert, was genau Gegenstand ist, welche Geschäftsprozesse, welcher Informationsverbund geschützt werden sollen. Im zweiten Schritt schafft die Organisation grobe Startbedingungen: Die Leitungsebene stellt benötigte Ressourcen bereit, benennt Rollen und standardisiert IT-Service-Prozesse. In Schritt 3 und damit sehr früh im RS7-Zyklus steht die Sensibilisierung der Mitarbeiter an. Sensibilisierte, aufmerksame Mitarbeiter, die sicherheitsrelevante Auffälligkeiten erkennen können und wissen, wie sie damit umgehen und welche Stellen sie kontaktieren sollen, bringen eine beträchtliche Sicherheitserhöhung mit sich.

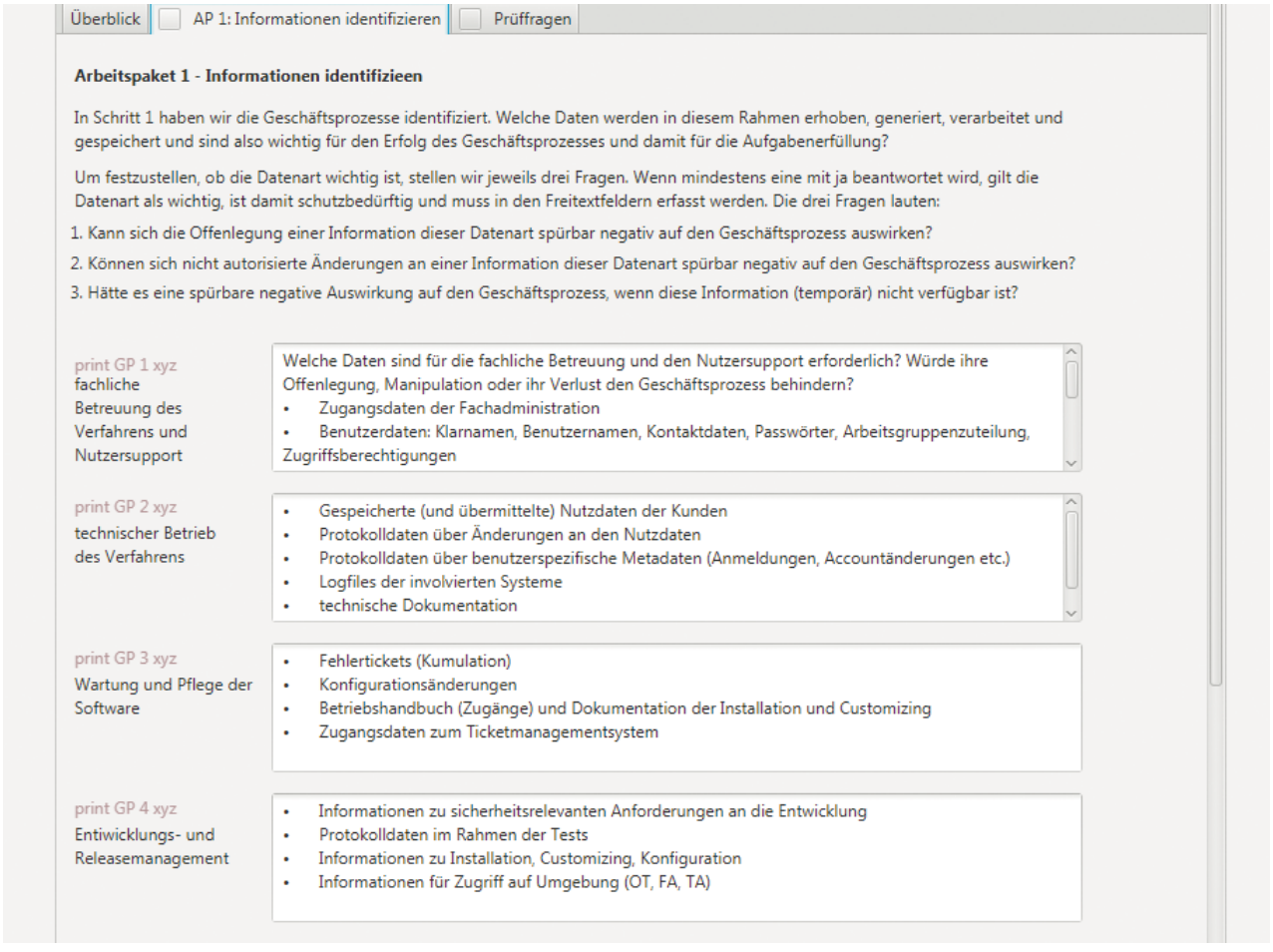

Abbildung 2: In Schritt 4 werden mit dem RS7-Tool pro Geschäftsprozess schützenswerte Informationen ermittelt.

Anschließend (Schritt 4) werden die kritischen Daten identifiziert. Welche Informationen sind so wichtig für den Geschäftsprozess, dass sie nicht verloren, verändert oder offengelegt werden dürfen? Schritt 5 leitet daraus die Schutzobjekte ab, auf denen die kritischen Daten verarbeitet oder gespeichert werden. Für diese Schutzobjekte werden dann im nächstenSchritt (Schritt 6) spezifische Sicherheitsmaßnahmen gemäß dem RS7-Maßnahmenkatalog umgesetzt. Im siebten optionalen Schritt wird der Abschluss des RS7-Prozesses durch ein Zertifikat bestätigt.

Ein eigens dafür entwickeltes Tool begleitet die Umsetzung von RS7. Es unterstützt alle Schritte mit Erklärungen, Beispielen und Hilfsmitteln, sodass der gesamte Prozess darin verfolgt und verwaltet werden kann.

Abbildung 3: Am Ende jeden Schrittes prüft das RS7-Tool, ob der Schritt vollständig abgeschlossen wurde.

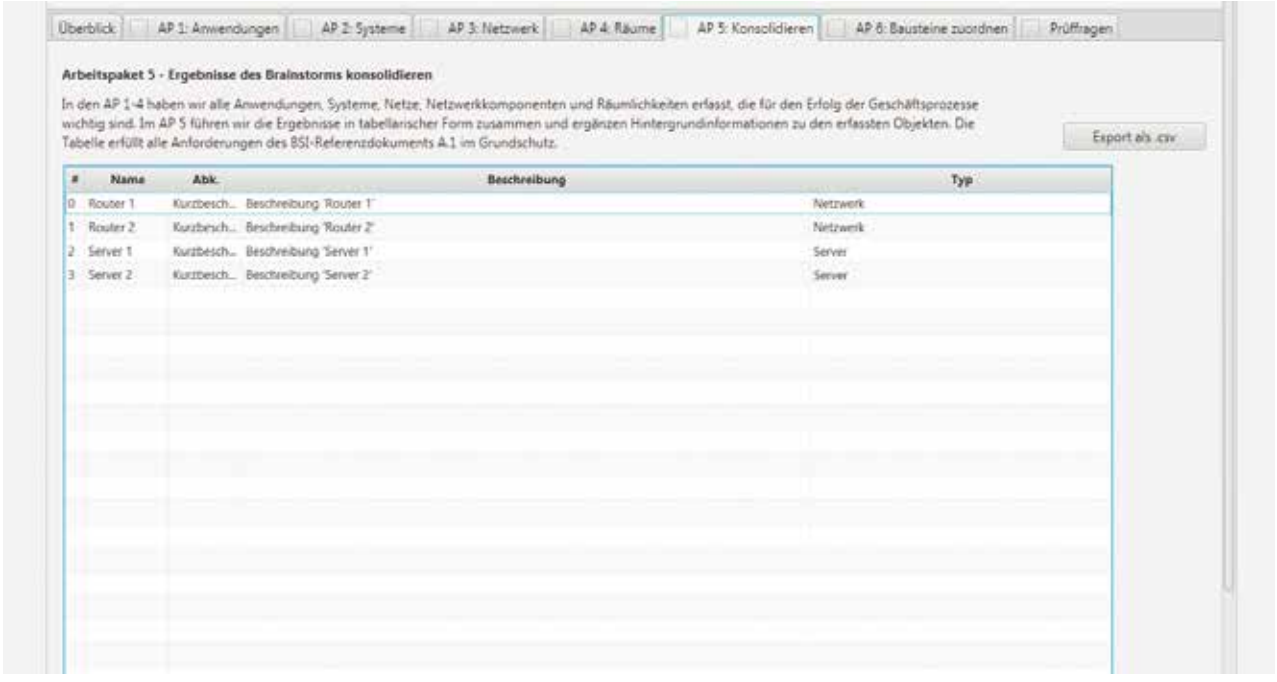

Abbildung 4: Eine BSI-konforme Tabelle im RS7-Tool listet alle Objekte auf, auf denen schützenswerte Daten verarbeitet werden.

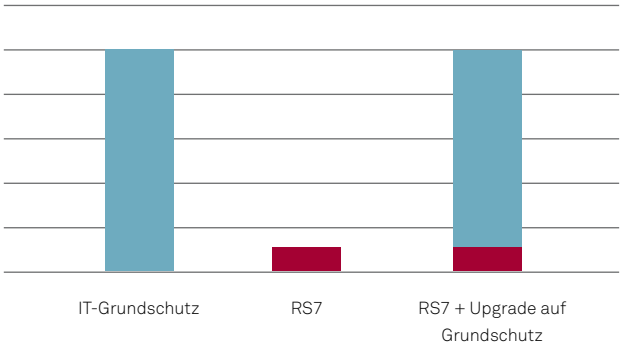

Abbildung 5: Aufwände für RS7 und IT-Grundschutz im Vergleich

Zwar wird mit RS7 nicht das Schutzniveau erreicht, das der IT-Grundschutz bietet, und das RS7-Zertifikat ist kein ISO-27000-Zertifikat – doch der große Vorteil von RS7 ist, dass es schnell, schlicht, kostengünstig und effektiv bei der Konzeptionierung einer Basissicherheit unterstützt (siehe Abbildung 5: Aufwände RS7 und IT-Grundschutz im Vergleich).

Darüber hinaus ist das RS7-Konzept in hohem Maße mit dem IT-Grundschutz des BSI kompatibel: Ein Sicherheitskonzept nach RS7 kann auf IT-Grundschutzlevel gehoben werden, ohne dass die Erstellung des RS7-Zertifikates zu obsoleten oder redundanten Mehraufwänden geführt hat. Die im RS7-Tool generierten Unterlagen sind BSI-konform und können direkt weiterverwendet werden.

FAZIT

Auch bei RS7 ist Sicherheit kein Projekt, sondern ein Prozess. Sind die sieben Schritte durchlaufen, haben sich mindestens die Umwelt und damit auch die relevanten Risiken verändert – und sich möglicherweise auch der zu schützende Verbund weiterentwickelt. An dieser Stelle kann das Sicherheitskonzept nach RS7 mit einer zweiten Runde durch den RS7-Zyklus fortgeschrieben oder nahtlos auf IT-Grundschutz umgesattelt werden.

RS7 will also keine Alternative zum IT-Grundschutz sein, sondern bietet als Vorstufe einen geschmeidigen Einstieg in die vielschichtige Thematik der Informationssicherheit. Wichtige und sensible Daten können recht schnell mit relativ niedrigem Ressourceneinsatz vor unspezifischen Bedrohungen geschützt werden. ●

ANSPRECHPARTNER FÜR RS7 – JENS WESTPHAL
Abteilungsleiter
Public Sector Security Consulting