

Erst Planen, dann schützen

Die zehn häufigsten Fehler in BSI IT-Grundschutz Projekten

Michael J. Gruber, Senior IT-Security Consultant, BSP.SECURITY

2009 wurde der BSI IT-Grundschutz 15 Jahre alt. Untersucht man die Realisierung von BSI IT-Grundschutz Projekten, zeigen sich eine Reihe typischer potenzieller Probleme. Welche Kardinalfehler können vermieden werden, um IT-Security Projekte erfolgreich abzuschließen? Und welche konkreten Maßnahmen helfen dabei, die Gefährdungen zu vermeiden?

Vergleicht man die Einführung eines ERP-Systems mit dem Aufbau eines Informationssicherheits-Management-Systems (ISMS) im Rahmen eines BSI IT-Grundschutzprojektes nach ISO 27001, so treten verschiedene Unterschiede deutlich zu Tage: Beim ERP-Projekt finden sich in der Regel klar definierte Projektziele, die in einem Projektzeitplan strukturiert sind. Eine ausreichende Unterstützung durch die Unternehmens-/Behördenleitung ist gewährleistet, externe Berater steuern das Projekt oder stehen zumindest beratend zur Seite und die Ausbildung der Anwender sorgt für Transparenz und Motivation.

Bei IT-Grundschutz Projekten besteht die Gefahr, dass die im Folgenden aufgeführten typischen Fehlerquellen den Projektablauf negativ beeinträchtigen oder sogar das Projekt in Gänze zum Scheitern bringen. Die angeführten Punkte basieren auf Erfahrungen unserer langjährigen Arbeit als Beratungsunternehmen im IT-Sicherheitsumfeld. Es handelt sich um einerseits generelle projektypische Fehlerquellen als auch um spezifische Fehlermuster bei der Umsetzung der BSI Security Standards:

1. Unklare Zielformulierung

Es gibt keine schriftlich fixierten und somit überprüfbareren Projektziele. Als Ziel wird lediglich vage die Verbesserung der IT-Security vereinbart. Fragt man Mitglieder des Projektteams, so werden unterschiedliche Ziele formuliert, die von den Erwartungen der Behörden-/



Michael J. Gruber ist Senior IT-Security Consultant bei BSP.SECURITY

Unternehmensleitung stark differieren können.

Empfehlung: Eine schriftliche Festlegung der Projektziele muss zum Start des IT-Security Projektes vorliegen: Was soll, bis wann, durch wen und wie konkret erzielt werden.

2. Mangelnde Erfahrung in der Projektarbeit

Der Projektverantwortliche, soweit dieser überhaupt explizit benannt worden ist, verfügt nicht über die notwendige Erfahrung, um ein derartiges Vorhaben mit allen damit verbundenen Aufgabenstellungen zu managen.

Empfehlung: Die Besetzung der Projektleitung muss sorgfältig erfolgen. Externe Beratung kann bei der richtigen Entscheidung helfen.

3. Keine klare Definition des zu untersuchenden Informationsverbundes

Die im BSI Standard 100-2 geforderte klare Definition des Informationsverbundes, also des Untersuchungs-

gegenstandes selbst, ist nicht klar formuliert und schriftlich fixiert. Für welche Bereiche der Organisation soll eine ISMS aufgebaut und eine entsprechende Sicherheitskonzeption erstellt werden?

Empfehlung: Eine schriftliche Fixierung des zu untersuchenden Informationsverbundes ist bei Projektbeginn vorzunehmen. Diese Definition wird von den Projektmitgliedern und der Organisationsleitung per Unterschrift verbindlich vereinbart.

4. Mangelhafte Unterstützung durch die Behörden-/Unternehmensleitung

Die Leitung der Organisation unterstützt das IT-Security Projekt nicht ausreichend mit Ressourcen und Mitteln. Entweder weil die notwendigen Ressourcen vom Projektteam nicht realistisch geplant oder nicht adäquat eingefordert wurden. Möglicherweise unterstützt die Organisationsleitung das Projekt auch nicht ausreichend.

Empfehlung: Festlegung und Genehmigung der benötigten Ressourcen zum Projektstart. Falls noch nicht geschehen, wird eine Informationssicherheitsleitlinie erstellt. In dieser wird auf die notwendige Unterstützung mit erforderlichen Ressourcen Bezug genommen. Wie in den BSI Standards 100-1 und 100-2 gefordert, ist diese zentrale Leitlinie von den Mitgliedern der Führungsebene zu unterschreiben.

5. Mangelnde Kenntnisse der BSI-Standards und Methodik

Die Mitglieder des Projektteams haben Defizite im Verständnis und der Anwendung der BSI-Stan-

dards und der damit verbundenen Methodik. Speziell der Aufbau eines ISMS wird nicht als notwendig erachtet. Bereits die ersten Projektarbeiten beginnen beim unstrukturierten Basis-Sicherheitscheck, ohne jedoch zuvor die notwendigen Basisarbeiten erledigt zu haben. Bei der Realisierung der Sicherheitskonzeption werden anstatt der breitenwirksamen A-Maßnahmen zuerst die C-Maßnahmen priorisiert, etc.

Empfehlung: BSI IT-Grundschutz ist mehr als nur die bekannten IT-Grundschutzkataloge. Die Projektmitglieder werden zu Projektbeginn im Rahmen einer Schulung mit den BSI Standards 100-1, 100-2 und 100-3 vertraut gemacht. Zudem wird der sinnvolle Einsatz eines entsprechenden Tools praxisnah erlernt (BSI Entwicklung „GSTOOL“, OpenSource-Lösung „verinice“ o.ä.).

6. Nur marginale Unterstützung durch externe Berater

Aus verschiedenen Gründen werden externe Berater zunächst nicht am Projekt beteiligt. Beratung wird erst dann zum Thema, wenn sich das IT-Security Projekt in einer „Sackgasse“ befindet.

Empfehlung: Durch Einbeziehung erfahrener IT-Security Consultants werden kostspielige Fehlentscheidungen im Projektverlauf vermieden. Durch Beratung, die bereits zu Beginn des Projektes einsetzt, kann der Ablauf realistisch strukturiert werden.

7. Projekt wird als „Undercover-Projekt“ ausgeführt

Projekte werden nicht offiziell betrieben, sondern ohne offiziellen Projektauftrag gestartet. Die Probleme mangelnder Ressourcen-Ausstattung sind hier vorprogrammiert. Eine notwendige Unterstützung durch Abteilungen der Organisation ist ohne offiziellen Auftrag nur schwer zu bekommen. Die Motivation der Initiatoren dieser IT-Sicherheits-Initiative wird rasch verfliegen, die Erfolgsaussichten auf einen erfolgreichen Abschluss sind schlecht.

Empfehlung: Versuchen Sie einen offiziellen Auftrag mit entsprechender Unterstützung der Organisationsleitung zu bekommen. Wenn Sie sich als interner Mitarbeiter nicht durchsetzen können, hilft unter Umständen die Präsentation durch externe Sicherheitsexperten vor der Organisationsleitung. Eine organisationsübergreifende Informationssicherheitsleitlinie dokumentiert die Wichtigkeit des Sicherheitsprojektes im Rahmen der allgemeinen Organisationsziele.

8. Keine definierten Meilensteine oder Projekt-Review

Es gibt keine klar definierten Meilensteine zur Kontrolle von Teilzielen. Somit sind eventuell notwendige Anpassungsarbeiten im Projektverlauf nicht möglich. Die Gefahr, dass das Security-Projekt aus dem Ruder läuft ist sehr hoch.

Empfehlung: Legen Sie schriftlich Termine für die Überprüfung von Teilzielen fest. Zu bestimmten Milestones wird der Verlauf des Projektes gemessen und gegebenenfalls entsprechend angepasst. Die Bewertung kann auch durch externe Berater erfolgen.

9. Ganzheitliche Sicht wird nicht erkannt

Ein BSI IT-Grundschutz Projekt umfasst wesentlich mehr als nur technische Aspekte. Speziell der Bereich Organisation wird oft ausgeklammert oder nur am Rande bearbeitet. Dies ist auch an Sicherheitsrichtlinien abzulesen, die durch ihren technischen Charakter Anwender nicht verständlich aufklären.

Empfehlung: Vermeiden Sie eine Fixierung auf die rein technischen Aspekte. IT-Security ist ein fortlaufender Prozess, der in einer Organisation ganzheitlich zu betrachten ist. In der BSI IT-Grundschutz Vorgehensweise wird diesem Punkt durch 15 Bausteine der Schicht 1 (Übergreifende Aspekte) ausdrücklich Rechnung getragen. Differenzieren Sie bei der Erstellung technischer/organisatorischer Sicherheitsrichtlinien und Benutzerleitfäden, indem Sie zielgruppengerecht formulieren.

10 Widerstände in der Organisation mangels fehlender Transparenz

Ohne Einbeziehung aller Mitarbeiter und die entsprechende Ausstattung mit Ressourcen wie in der offiziellen Informationssicherheitsleitlinie definiert, fehlt die notwendige Transparenz und somit die notwendige Unterstützung im Laufe des Projektes. Anwender werden nicht selten mit Maßnahmen im Security-Bereich konfrontiert, ohne deren Sinn verstehen zu können. Dies trifft für technische aber auch für organisatorische Modifikationen zu.

Empfehlung: Alle Mitarbeiter müssen laufend über das IT-Security Projekt ausreichend und zielgruppengerecht informiert werden. Das Thema lässt sich durch den Einsatz verschiedener Medien entsprechend aufbereiten. Ohne ausreichende Einbeziehung und Motivation aller Mitarbeiter einer Organisation bleibt der Faktor Mensch ein Risikofaktor.

Fazit

Viele BSI IT-Grundschutz Projekte müssen während ihrer Laufzeit „saniert“ werden. Die angeführten Fehlerquellen sind eine potenzielle Gefährdung für einen positiven Projektabschluss. In den meisten Fällen gelingt es, dem Projekt durch eine offene Analyse wieder Schwung und Richtung zu geben. IT-Security Projekte kosten Geld, aber noch mehr kostet es, ein Projekt zu sanieren oder bestimmte Aufwände mehrfach zu zahlen. Deshalb ist eine realistische Planung im Vorfeld und eine gezielte kontinuierliche Projektbegleitung so wichtig für die erfolgreiche, nachhaltige und ganzheitliche Umsetzung.