IT-SECURITY

IT-Grundschutzzertifikat

Sicherheit mit Brief und Siegel!

Alexander Geschonneck
Timo Kob
Lizensierte Grundschutzauditoren
HiSolutions AG

Mit dem steigenden Bewusstsein für IT-Sicherheit wuchs in den letzten Jahren der Bedarf, ein Prüfsiegel zu schaffen, mit dem das eigene Sicherheitsniveau dokumentierbar ist. Nachdem hier das British Standards Institution frühzeitig die Zeichen der Zeit erkannt und eine Zertifizierung gemäß des BS7799-Standards ermöglicht hatte, trug im Jahre 2002 auch das Bundesamt für die Sicherheit in der Informationstechnik (BSI) den vielfachen Wünschen aus der Industrie und Verwaltung Rechnung und schuf mit dem IT-Grundschutzzertifikat auf Basis des IT-Grundschutzhandbuchs (GSHB) ein eigenes Zertifikat.

Handelt es sich bei der BS7799 (und dem internationalen Pendant ISO17799) um allgemeingültigere Vorgaben zum Aufbau eines Security Managements, so ist das GSHB eine in regelmäßigen Abständen aktualisierte Loseblattsammlung, die neben mit dem BS7799 vergleichbaren Anforderungen für ein Security Management konkrete Maßnahmen für die behandelten Plattformen enthält. So ermöglicht es eine zügige und kosteneffektive Lösung häufiger Probleme und hilft das allgemeine Sicherheitsniveau - bei wirtschaftlichem Ressourceneinsatz - zu erhöhen. Der Grundschutzansatz ermöglicht durch einen einfachen Soll-Ist-Vergleich eine effektive und wirtschaftliche Arbeitsweise. Es werden in den einzelnen Kapiteln kompakte Sicherheitskonzepte zur Adaption an das eigene Umfeld angeboten. Die empfohlenen Maßnahmen weisen durch ihre Praxiserprobung eine hohe Wirksamkeit auf. Grundschutzmaßnahmen sind meist - da stark verbreitet und in einer Vielzahl vergleichbarer Organisationen im Einsatz - relativ kostengünstig und schnell zu implementieren. Der Einsatz des GSHB führt somit schnell zu einem relativ hohen Niveau an Sicherheit gegen die häufigsten Bedrohungen.

BS7799 oder IT-Grundschutzzertifikat?

Grundsätzlich gilt, dass beide Standards und Zertifizierungen auch weiter ihre Berechtigung haben. So werden international agierende Unternehmen ggf. weiter zum BS7799-Zertifikat tendieren, da dieses international einen höheren Bekanntheitsgrad hat. Hinzu kommt, dass mit dem IT-Grundschutzzertifikat nur Strukturen geprüft werden können, deren zentrale Komponenten auch im GSHB berücksichtigt sind. Beinhaltet ein Untersuchungsgegenstand Systeme und Anwendungen, die für die Mehrheit der Kernaufgaben unterstützend sind und kein entsprechender Baustein aus dem GSHB verfügbar ist (z.B. AS/400 oder OS/390), kann kein Zertifikat erstellt werden. Der allgemein gehaltene BS7799 kennt solche Restriktionen nicht. Umgekehrt bewirken die konkreteren Anforderungen des GSHB und das über das Security Management hinausgehende Prüfumfeld für viele eine repräsentativere Aussage über die vorhandene Gesamtsicherheit. Da eine große Anzahl von Unternehmen (nicht nur in Deutschland!) sich bei der Erstellung ihrer Sicherheitskonzepte ohnehin an das GSHB zumindest anlehnt, ist eine hierauf basierende Zertifizierung zumindest für diese Unternehmen ein logischer Schritt. Weitere Vorteile der IT-Grundschutzzertifizierung sind das Stufenmodell, das einen schnellen Einstieg durch Selbsterklärungen ermöglicht, sowie die Tatsache, dass auf der Urkunde explizit auf die Erfüllung der Kriterien der ISO17799 hingewiesen wird. Somit ist also auch für internationale Kontakte, die das GSHB nicht kennen, ein erkennbares Qualitätskriterium durch das Grundschutzzertifikat gegeben.

Das Zertifizierungs-Projekt

Das BSI definiert drei unterschiedliche Ausprägungen der Qualifizierung nach IT-Grundschutz. Es werden gewissermaßen zwei Vorstufen zum eigentlichen Zertifikat angeboten. Mit diesen als Selbsterklärung bezeichneten Vorstufen können bereits umgesetzte Maßnahmen schrittweise dargestellt werden, ohne den Aufwand für eine vollständige Zertifizierung zu treiben. Eine Selbsterklärung kann in der erreichten Form nicht wiederholt werden. Nach

GIT Sicherheit + Management 2/2003, S. 60–61, GIT VERLAG GMBH & Co. KG, Darmstadt, www.gitsicherheit.de

Ablauf der Selbsterklärung muss immer die nächst höhere Stufe des Qualifizierungsschemas erlangt werden.

Häufigstes Missverständnis im Vorfeld einer Zertifizierung ist der Glaube, dass die gesamte IT-Struktur eines Unternehmens zertifiziert werden muss. Dies ist nicht richtig. Zertifizierbar sind sog. IT-Verbünde, d.h. sauber abgrenzbare Teilstrukturen. Abgrenzbar gilt hier sowohl für die Technik als auch für die zugrundliegenden Geschäftsprozesse. Zertifizierbar sind eine oder mehrere Fachaufgaben, Geschäftsprozesse oder Organisationseinheiten. Um hier keine unliebsamen Überraschungen in beide Richtungen zu erleben, gilt es, von Anfang an die Zertifizierbarkeit des geplanten Untersuchungsgegenstands zu gewährleisten. Dies bedeutet beispielsweise sicherzustellen, dass für die zentralen Komponenten überhaupt Grundschutzmaßnahmen existieren oder die komplette Abdeckung der relevanten Geschäftsprozesse durch die zu überprüfenden System zu verifizieren.

Anschließend sollte in einer ersten Kurz-Analyse grob der erforderliche Aufwand bis hin zur Erfüllung der jeweiligen Zertifizierungsstufen ermittelt, so dass eine ökonomische und aus Sicherheitssicht sinnvolle Roadmap aufgezeigt werden kann. Steht nicht bereits von Anfang an fest, welche Zertifizierungsstufe im ersten Schritt angestrebt werden soll, so dient diese erste Analyse als Entscheidungshilfe für die Auswahl des Projektzieles.

Da diese beiden Grundsatzentscheidungen entscheidenden Einfluss auf den weiteren Fortgang des Projektes haben, ist es sinnvoll, bereits hier die Unterstützung eines lizenzierten Auditors in Anspruch zu nehmen. Es gilt aber zu bedenken, dass dieser dann nicht die eigentliche Zertifizierung durchführen kann, da der Auditor in den letzten 2 Jahren vor der Prüfung nicht beratend im Hause des Zertifikats-Antragsstellers tätig gewesen sein darf. Wichtig ist diese frühzeitige Einbindung vor allem auch bei der Definition der für die Zertifizierung nicht erforderlichen Grundschutz-Maßnahmen. Für alle als entbehrlich markierten Maßnahmen muss eine stichhaltige und nachvollziehbare Begründung existieren.

Die Ergebnisse der zuvor durchgeführten Kurzanalyse gehen dann in das Herzstück der Vorarbeiten, den Basis-Sicherheitscheck ein. Hier wird mithilfe von Interviews der jeweiligen Ansprechpartner exakt der Status der erforderlichen Standard-Sicherheitsmaßnahmen aufgenommen und das konkrete weitere Vorgehen bis hin zur eigentlichen Zertifizierung festgelegt. Sollten sich hier in die eine oder andere Richtung größere Abweichungen von den ersten Annahmen ergeben, so ist hier noch die Erhöhung oder Absenkung des Zertifizierungsniveaus möglich. Der letzte Akt der Vorbereitung besteht in der Anmeldung zur Zertifizierung beim BSI.

Das Testat

Nur in der höchsten Stufe, dem IT-Grundschutzzertifikat, ist der Einsatz eines lizenzierten Auditors zwingend erforderlich. Man kann aber die Wertigkeit der Selbsterklärungen durch ein Testat eines solchen Prüfers deutlich erhöhen. Im Unterschied zur eigentlichen Zertifizierung entfällt aber weiterhin die Überprüfung durch das BSI, so dass ein solches Testat ohne weitere Lizenzierungsgebühren und innerhalb eines kurzen Zeitraumes erreichbar ist. Da das Testat die – subjektive – Wertigkeit der Selbsterklärung mit nur minimalem Mehraufwand signifikant erhöht, ist dieser Schritt in jedem Fall empfehlenswert.

Zertifizierung

Die eigentliche Auditierung besteht aus einer Plausibilitätsprüfung, in der die Zertifizierbarkeit des Prüfungsgegenstandes kontrolliert wird, und der anschließenden stichprobeweisen Realisierungsprüfung. Findet der Auditor Mängel, die eine Zertifizierung verhindern, so hat das Unternehmen die Möglichkeit der Nachbesserung, ohne dass sich dies auf die abschließende Aussage auswirkt. Erst nach einer zweimaligen erfolglosen Nachbesserung muss das Zertifizierungsprojekt abgebrochen und ein neuer Antrag beim BSI gestellt werden. Eigentlich selbstverständlich aber dennoch oft nachgefragt ist der Punkt, dass keine geschäftsrelevanten Informationen oder Geschäftsdaten das Unternehmen verlassen. Auch das BSI erhält nur die zur Prüfung erforderlichen Informationen (z.B. einen Netzplan des Prüfgegenstandes) und z.B. keinen direkten Zugang zu den Systemen.

Mit dem IT-Grundschutz-Zertifikat werden verschiedene Zielgruppen angesprochen. Damit wird zum Vertrauensgewinn beigetragen, indem nachgewiesen wird, dass IT-Sicherheit nach IT-Grundschutz umgesetzt ist und aufrechterhalten wird. Die Möglichkeit, einen Nachweis für ein definiertes Sicherheitsniveau zu erbringen, macht die Bestrebungen für IT-Sicherheit transparent.

Weitere Informationen hierzu finden sie z.B. unter www.grundschutzhandbuch.de.