

Ralph Lehmann
IT-Sicherheitsanalyse
und Beratung

Ralph Lehmann
IT-Sicherheitsanalyse
und Beratung

Ralph Lehmann · IT-Sicherheitsanalyse und Beratung · Kochstraße 34 · 04275 Leipzig

Kochstraße 34
04275 Leipzig

Tel.: (03 41) 3 06 99 05
Fax: (03 41) 3 08 10 31
mobil: (01 70) 3 11 37 35

e-mail: info@ralph-lehmann.de
Web: www.ralph-lehmann.de

Überblick zur Einrichtung und Aufrechterhaltung der IT-
Sicherheit gem. Grundschutzhandbuch (GSHB)
des Bundesamtes für Sicherheit in der Informationstechnik
(BSI)

Die folgenden Ausführungen stützen sich im Wesentlichen auf das Beispielprofil des BSI für mittelständische Unternehmen. Dieses Dokument kann unter

http://www.bsi.bund.de/gshb/deutsch/hilfmi/profil_mittl_IT_Verbund.pdf

kostenlos herunter geladen werden.

Das Beispielprofil setzt die Kenntnis des "Leitfadens IT-Sicherheit" voraus, welcher unter

<http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf>

ebenfalls kostenlos heruntergeladen werden kann.

0. Fragen und Antworten

Wozu brauchen wir überhaupt eine Sicherheitsanalyse, obwohl bei uns bereits Sicherheitsprodukte¹ installiert sind?

Es ist nicht möglich, eine geeignete Auswahl an Sicherheitsmaßnahmen zu treffen, wenn die möglichen Gefährdungen des Gesamtsystems nicht bekannt sind. So kann z.B.

- ein Virenschanner nicht vor Schwachstellen des Betriebssystems schützen,
- eine Firewall fahrlässiges Verhalten der Benutzer nicht kompensieren,
- ein Backupsystem keine Verletzung des Datenschutzes oder das Ausspähen von Betriebsgeheimnissen verhindern,
- ein Proxyserver die Internetnutzung nicht sinnvoll einschränken, wenn Benutzer in der Lage sind, sich auch über ein Modem einzuwählen.

Es ist deshalb unabdingbar, die potentiellen Gefährdungen des Systems zu analysieren, bevor eine Auswahl darauf abgestimmter Abwehrmaßnahmen getroffen werden kann.

Welcher Schutz ist eigentlich "angemessen"?

Der Schutzbedarf orientiert sich an den möglichen Schäden, die mit der Beeinträchtigung einer betroffenen Komponente verbunden wären und wird in die drei Kategorien normal, hoch und sehr hoch unterteilt. Die angemessene Auswahl und Qualität der Schutzmaßnahmen sind direkt von diesem Schutzbedarf abhängig.

Zur Einstufung in diese Kategorien werden individuell für den betrachteten IT-Verbund die Auswirkungen hinsichtlich der Schadensszenarien

- finanzielle Schäden
- negative Außenwirkung (Imageschäden)
- Beeinträchtigung der Aufgabenerfüllung
- Verstoß gegen Gesetze, Vorschriften oder Verträge sowie daraus folgende straf- oder zivilrechtliche Konsequenzen
- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit

1) z.B. Firewall, Virenschanner, Backupprogramme usw.

betrachtet. Der Schutzbedarf wird wie folgt definiert:

- normal* - die Schadensauswirkungen sind begrenzt und überschaubar
- hoch* - die Schadensauswirkungen können beträchtlich sein
- sehr hoch* - die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen

Ist der Schutz nach Anwendung des GSHB ausreichend?

Ja, falls keine Komponente des IT-Verbundes einen hohen oder sehr hohen Schutzbedarf aufweist. Zusätzliche Maßnahmen (Differenz-Sicherheitsanalyse, Risikoanalyse, Penetrationstests etc.) sind nur bei erhöhtem Schutzbedarf notwendig.

Wie läuft die Anwendung des GSHB prinzipiell ab?

Der gesamte Prozess umfasst folgende Phasen:

- Initiierung des IT-Sicherheitsprozesses
- Erstellung einer Leitlinie
- Benennung eines internen Sicherheitsverantwortlichen
- optionale Beauftragung eines externen Sicherheitsverantwortlichen
- Durchführung einer IT-Strukturanalyse
- Durchführung der Schutzbedarfsfeststellung
- Modellierung des IT-Verbunds gem. GSHB
- Durchführung des Basis-Sicherheitschecks
- Realisierung bisher nicht umgesetzter IT-Sicherheitsmaßnahmen
- Zertifizierung (optional)

Diese Phasen werden in den Abschnitten 1 bis 7 näher beschrieben.

Ist nach Anwendung des GSHB 100%-ige Sicherheit garantiert?

Nein, die Sicherheit ist angemessen. Einige einfache zusätzliche Maßnahmen können diese weiter verbessern, ohne dass hierbei erhebliche Mehrkosten entstehen würden. Nur ausnahmsweise sind dagegen die erweiterten Methoden (Differenz-Sicherheitsanalyse, Risikoanalyse, Penetrationstests) notwendig.

Ist die Anwendung des GSHB eine einmalige Angelegenheit?

Das Verfahren sollte in regelmäßigen Abständen sowie nach signifikanten Änderungen im IT-Verbund wiederholt werden.

Was kostet uns die Anwendung des GSHB?

Ein erheblicher Teil der notwendigen Arbeiten wird von im IT-Verbund tätigen internen Mitarbeitern ausgeführt. Die Verbesserung der Sicherheit nach IT-Grundschutz ist deshalb ein sehr kostengünstiges Verfahren.

Natürlich ist die Beauftragung eines unabhängigen externen IT-Sicherheitsbeauftragten zunächst mit einem gewissen Aufwand verbunden. Hierdurch können jedoch weitaus höhere Kosten z.B. für

- unnötige Investitionen, Wartungsverträge etc.
- Schäden aufgrund übersehener Schwachstellen als Folge der gefürchteten "Betriebsblindheit"
- Schäden aufgrund unzureichender Sachkenntnis

vermieden werden.

Warum sollte die Sicherheitsanalyse nicht durch unseren IT-Dienstleister, mit dem wir schon lange gut zusammenarbeiten, durchgeführt werden?

Eine objektive Beurteilung Ihrer IT-Sicherheit ist nur dann möglich, wenn eine Kollision mit anderen Interessen des Auditors¹ (z.B. durch den Vertrieb von Komponenten, Dienstleistungen, Software etc.) nicht besteht. Einem durch das BSI zertifizierten Auditor¹ sind solche Tätigkeiten übrigens explizit untersagt.

1. Initiierung des IT-Sicherheitsprozesses

Die grundlegenden Voraussetzungen zur erfolgreichen Optimierung der Sicherheit in der IT sind

- die Definition eindeutiger Sicherheitsziele (IT-Sicherheits-Leitlinie)
- die Festlegung des/der Verantwortlichen für deren Umsetzung (IT-Sicherheitsbeauftragter)

Die Sicherheits-Leitlinie beschreibt das innerhalb des Geltungsbereiches (IT-Verbundes) angestrebte Sicherheitsniveau. Sie definiert daher einerseits den IT-Verbund, in dem sie gültig sein soll und andererseits die von der Institution angestrebten Sicherheitsziele.

Die Leitung der Institution informiert nach Erstellung der Leitlinie alle Mitarbeiter von deren Existenz und weist darauf hin, dass deren Einhaltung für die Institution von wesentlicher Bedeutung und deshalb für alle Mitarbeiter verbindlich ist.

Weiterhin benennt die Institution einen internen IT-Sicherheitsbeauftragten und ggf. einen externen IT-Sicherheitsbeauftragten. Falls das IT-Grundschutz-Projekt ohne externe Hilfe realisiert werden soll, trägt der interne Sicherheitsbeauftragte die gesamte Verantwortung für das Projekt.

Wird jedoch zusätzlich ein externer Sicherheitsspezialist beauftragt, reduziert sich die Verantwortung des internen Verantwortlichen i.d.R. auf die Bereitstellung notwendiger Daten, die Aufrechterhaltung der Kommunikation mit der Leitung der Institution und schließlich die Durchsetzung erforderlicher Maßnahmen.

1) die für die Überprüfung verantwortliche Person, also i.d.R. der externe Sicherheitsbeauftragte

2. IT-Strukturanalyse

Im Rahmen der IT-Strukturanalyse wird der IT-Verbund vollständig erfasst und alle Komponenten katalogisiert. Normalerweise wird die IT-Strukturanalyse vom IT-Sicherheitsbeauftragten (ggf. mit Unterstützung durch weitere IT-Verantwortliche) durchgeführt.

Die Analyse besteht aus den folgenden Schritten:

- Erstellung bzw. Aktualisierung und nachfolgende Auswertung des Netzwerkplans
- Erfassung der IT-Systeme, IT-Anwendungen und der zugehörigen Informationen

3. Schutzbedarfsfeststellung

Das Ziel dieses Schrittes ist die Bestimmung des Schutzbedarfs für alle Komponenten des IT-Verbunds. Da der Schutzbedarf meist nicht exakt quantifizierbar ist, beschränkt sich das GSHB auf eine pauschale Klassifizierung.

Jede einzelne Komponente wird einer der drei Kategorien – normal, hoch oder sehr hoch – zugeordnet. Hierbei ist die Orientierung an den drei Grundwerten der IT-Sicherheit Vertraulichkeit, Integrität und Verfügbarkeit von entscheidender Bedeutung.

4. Modellierung

Der betrachtete IT-Verbund wird mit Hilfe der so genannten Bausteine des IT-Grundschrifts nachgebildet. Jeder dieser Bausteine enthält eine Zusammenstellung einzelner Sicherheitsmaßnahmen. Als Ergebnis dieser Phase entsteht ein IT-Grundschriftmodell des IT-Verbunds, das aus verschiedenen, teilweise auch mehrfach verwendeten Bausteinen des GSHB besteht, die den einzelnen Objekten des IT-Verbunds zugeordnet sind.

Ergebnis der Modellierung ist schließlich eine Liste von Objekten und den diesen zugeordneten Sicherheitsmaßnahmen, deren Umsetzung im nächsten Schritt überprüft werden kann.

5. Basis-Sicherheitscheck

Der Basis-Sicherheitscheck hat das Ziel festzustellen, welche der durch das GSHB vorgegebenen Standardsicherheitsmaßnahmen bisher nicht oder nicht ausreichend umgesetzt sind. Die in der vorangegangenen Phase entstandene Zusammenstellung der zu verifizierenden Maßnahmen wird dabei als Prüfplan für einen Soll-Ist-Vergleich verwendet.

Bei konsequenter Abarbeitung aller laut GSHB empfohlener Überprüfungen ist hierbei sichergestellt, dass tatsächlich alle notwendigen Sicherheitsmaßnahmen entweder als bereits umgesetzt, entbehrlich oder aber als bisher nicht oder nicht ausreichend umgesetzt identifiziert werden.

6. Realisierung - Umsetzung von Sicherheitsmaßnahmen

Nach der Ausführung des Basis-Sicherheitschecks liegen alle Informationen vor, um die Umsetzung der bisher nicht oder nur teilweise realisierten Standardsicherheitsmaßnahmen zu planen.

Wurden während der Überprüfung nur wenige bisher nicht realisierte Maßnahmen identifiziert und bindet deren Umsetzung nur geringe finanzielle und personelle Ressourcen, kann oft unmittelbar entschieden werden, durch wen und bis wann diese Maßnahmen ausgeführt werden sollen. Im Falle von zahlreichen noch zu realisierenden Maßnahmen ist natürlich eine entsprechende Planung erforderlich.

7. Zertifizierung (optional)

Die Umsetzung der im GSHB beschriebenen Standardsicherheitsmaßnahmen kann mittels der so genannten Selbsterklärung bzw. eines vom BSI ausgegebenen IT-Grundschutz-Zertifikats gegenüber Dritten transparent gemacht werden. Durch die Veröffentlichung auf dem Webserver des BSI ist auch für Außenstehende erkennbar, dass sich eine Institution erfolgreich mit der eigenen IT-Sicherheit auseinandergesetzt hat.

Stand: 03.07.2006

Die jeweils aktuellste Version dieses Dokuments können Sie unter www.ralph-lehmann.de/Service_Downloads/service_downloads.html herunterladen.