

**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](mailto:info@ralph-lehmann.de)  
Web: [www.ralph-lehmann.de](http://www.ralph-lehmann.de)

## IT-Sicherheit kompakt

Vereinfachte Anwendung des Grundschutzhandbuchs (GSHB) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in kleinen Unternehmen

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

[http://www.bsi.bund.de/gshb/deutsch/hilfmi/profil\\_kl\\_institution.pdf](http://www.bsi.bund.de/gshb/deutsch/hilfmi/profil_kl_institution.pdf)

kostenlos heruntergeladen 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 Sicherheitsprodukte<sup>1</sup> 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 Virens scanner 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 angemessen? Ist die Anwendung des GSHB in einem kleinen Unternehmen nicht übertrieben?***

Der Schutzbedarf orientiert sich an den möglichen Schäden, die mit einer 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

1) z.B. Firewall, Virens scanner, Backupprogramme usw.

- Verstoß gegen Gesetze, Vorschriften oder Verträge sowie daraus folgende straf- oder zivilrechtliche Konsequenzen
- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit

betrachtet. Der Schutzbedarf wird wie folgt definiert:

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

Gerade in kleinen Unternehmen wird jedoch oft die Anwendung des GSHB selbst als unangemessen aufwändig angesehen und deshalb abgelehnt. In diesem Leitfaden soll deshalb eine Methode beschrieben werden, wie auch für kleine Unternehmen die Empfehlungen des GSHB bestmöglich mit minimalem Aufwand umgesetzt werden können.

### ***Ist der Schutz nach der vereinfachten Anwendung des GSHB ausreichend?***

Ja, falls keine Komponente des IT-Verbunds einen hohen oder sehr hohen Schutzbedarf aufweist.

Zusätzliche Maßnahmen (Differenz-Sicherheitsanalyse, Risikoanalyse, Penetrationstests etc.) sind nur bei erhöhtem Schutzbedarf notwendig.

Bei der im Folgenden vorgestellten Herangehensweise wird von Anfang an davon ausgegangen, dass alle Komponenten lediglich einen normalen Schutzbedarf aufweisen. Eine gesonderte Schutzbedarfsfeststellung entfällt.

### ***Wie läuft die vereinfachte Anwendung des GSHB prinzipiell ab?***

Der gesamte Prozess umfasst folgende Phasen:

1. Initiierung des IT-Sicherheitsprozesses
  - Übernahme einer bewährten Standard-Sicherheitsleitlinie
  - Benennung eines internen Sicherheitsverantwortlichen
  - optionale Beauftragung eines externen Sicherheitsverantwortlichen
2. Durchführung einer IT-Strukturanalyse
3. Pauschale Festlegung des Schutzbedarfs auf *normal*
4. Modellierung des IT-Verbunds gem. GSHB
5. Durchführung des Basis-Sicherheitsschecks
6. Realisierung bisher nicht umgesetzter IT-Sicherheitsmaßnahmen

Diese Phasen werden in den Abschnitten 1 bis 6 näher vorgestellt.

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

Nein, die Sicherheit ist angemessen. Durch die vereinfachte Anwendung des GSHB können Mängel im Einzelfall unentdeckt bleiben.

### ***Ist die vereinfachte Anwendung des GSHB eine einmalige Angelegenheit?***

Das Verfahren sollte in regelmäßigen Abständen sowie nach signifikanten Änderungen im IT-Verbund wiederholt werden. Sollte der IT-Verbund wesentlich vergrößert werden ist eine reguläre Anwendung des GSHB empfehlenswert.

### ***Was kostet uns die vereinfachte Anwendung des GSHB?***

Ein erheblicher Teil der notwendigen Arbeiten wird von im IT-Verbund tätigen internen Mitarbeitern ausgeführt. Die Verbesserung der Sicherheit durch die Anwendung des GSHB 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 wie z.B. für

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

vermieden werden. Durch die Vereinfachung einzelner Schritte gegenüber dem regulären Verfahren werden die Kosten nochmals gesenkt.

### ***Warum sollte die Herstellung der Sicherheit nicht durch unseren IT-Dienstleister, mit dem wir schon lange gut zusammenarbeiten, durchgeführt werden?***

Eine objektive Beurteilung Ihrer Sicherheit ist nur dann möglich, wenn eine Kollision mit anderen Interessen des Auditors<sup>1</sup> (z.B. durch den Vertrieb von Komponenten, Dienstleistungen, Software etc.) nicht besteht. Einem durch das BSI zertifizierten Auditor<sup>1</sup> sind solche Tätigkeiten sogar explizit untersagt. Im Übrigen stehen die notwendigen benutzerdefinierten Bausteine des GSHB Ihrem Dienstleister nicht zur Verfügung.

### ***Welche Voraussetzungen muss ein Unternehmen für die kompakte Anwendung des GSHB erfüllen?***

- max. 4 im IT-Verbund verwendete Computer
- max. 4 an diesen Computern arbeitende Personen
- ausschließlich Windows 2000 oder XP als Betriebssystem
- keine Dienste (z.B. Webserver, Mailserver, Fernwartung etc.), welche nach außen angeboten werden
- keine Computer, die außer im Firmenverbund in weiteren Netzwerken betrieben werden (z.B. Laptops, die auch im Homeoffice verwendet werden)
- nur Standardnetzwerk (Ethernet oder WLAN)

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

- keine Speicherung vertraulicher/personenbezogener Daten
- keine gesetzliche Verpflichtung zur Geheimhaltung

## **1. Initiierung des IT-Sicherheitsprozesses**

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.

Bei der vereinfachten Anwendung des GSHB wird im Rahmen dieses Schrittes lediglich eine bewährte Standard-Sicherheitsleitlinie als verbindlich erklärt.

Ferner wird ein interner Sicherheitsbeauftragter benannt, falls diese Funktion nicht durch den Unternehmer selbst abgedeckt wird.

## **2. IT-Strukturanalyse**

Im Rahmen der IT-Strukturanalyse wird der IT-Verbund vollständig erfasst und alle Komponenten katalogisiert. 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-Grundschutzhandbuchs nachgebildet. Jeder dieser Bausteine enthält eine Zusammenstellung einzelner Sicherheitsmaßnahmen. Als Ergebnis dieser Phase entsteht ein IT-Grundschutzmodell 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.

Stand: 26.06.2005

Die jeweils aktuellste Version dieses Dokuments können Sie unter [www.ralph-lehmann.de/Service\\_Downloads/service\\_downloads.html](http://www.ralph-lehmann.de/Service_Downloads/service_downloads.html)

herunterladen.