Sicherheitsleitfaden für Applicaton Service Providing

BITKOM
Connecting visions - creating solutions

Impressum

Herausgeber:
BITKOM
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.
Albrechtstraße 10
10117 Berlin-Mitte

Tel.: 030/27 576 – 0
Fax: 030/27 576 – 400
bitkom@bitkom.org
www.bitkom.org

Redaktion:	Dr. Stefan Schröder, Dr. Axel Garbers
Verantwortliches BITKOM-Gremium:	Arbeitskreis Application Service Providing
Redaktionsassistenz:	Jana Rings, BITKOM e.V.
Stand:	März 2006

Ansprechpartner:
Dr. Axel Garbers, BITKOM e.V.
Tel: +49 (0)30 / 27576 – 244
E-Mail: a.garbers@bitkom.org

Inhaltsverzeichnis

Management Summary

Der Angeber kommt meist nicht weit.
Es fehlt ihm ja die Sicherheit,
mit der - ganz ohne anzugeben -
die wahrhaft Fortgeschritt'nen leben.

Wilhelm Busch
(1832 - 1908), deutscher Zeichner, Maler und Schriftsteller

Wer hat diesen Leitfaden erstellt?

Der BITKOM Arbeitskreises ASP (Application Service Providing) setzt sich aus Vertretern unterschiedlicher Firmen aus den Bereichen Informationstechnologie und IT–Dienstleistung zusammen. Er hat sich zum Ziel gesetzt für Anbieter und Kunden Orientierungshilfen zu erarbeiten, die als Grundlage der Zusammenarbeit in einem so genannten ASP-Modell dienen können, also einem Servicemodell, das gemeinhin als „Software als Service“ oder „Software aus der Steckdose“ bezeichnet wird. Neben dem hier vorliegenden Sicherheitsleitfaden wurde bereits ein Mustervertrag für ASP-Leistungen erarbeitet, der als Rahmen und Grundlage einer Leistungsvereinbarung zwischen Anbietern und Kunden herangezogen werden kann.

Wozu soll dieser Leitfaden dienen?

Neben den Anforderungen an die Funktionalität und Verfügbarkeit einer Anwendung spielen bei ASP-Angeboten die Betriebs- und Datensicherheit sowie der Schutz der Daten eine herausgehobene Rolle. Wie stellt der Anbieter sicher, dass meine Daten auf dem Kommunikationsweg und bei der Verarbeitung im zentralen Rechenzentrum des Anbieters unverfälscht bleiben, vertraulich behandelt und sicher aufbewahrt werden. Was muss der Kunde dazu beitragen, dass Zugangs- und Zugriffssicherheit auf Systeme und Daten lückenlos gewährleistet werden kann. Der Leitfaden soll als Instrument zur gegenseitigen Prüfung und Kontrolle aller sicherheitsrelevanten Aspekte der Datenverarbeitung dienen und so helfen das Kundenvertrauen in die Leistungsfähigkeit der angebotenen ASP-Lösung zu stärken.

An wen richtet sich dieser Leitfaden?

Der Sicherheitsleitfaden wendet sich an Sicherheits- und IT-Spezialisten bei **ASP-Anbietern** und gibt ihnen eine Hilfestellung zur Strukturierung der Sicherheitsanalyse. Insbesondere macht er deutlich, dass Sicherheit nicht an den Grenzen der Systeme des Anbieters aufhört, sondern ohne Mitwirkung des Kunden nicht gewährleistet werden kann. Für **Kunden** bietet der Leitfaden eine Hilfestellung hinsichtlich der trotz ASP-Modell notwendigen Sicherheitsvorkehrungen im eigenen Verantwortungsbereich.

Wie ist der Leitfaden aufgebaut?

Nach einer kurzen Einleitung strukturiert der Leitfaden das Thema Sicherheit in zwei Dimensionen: Verantwortlichkeiten (Kunden / Anbieter) und verwaltete Objekte (Infrastruktur, Endgeräte, Netze, ASP-Server, Daten). Für die Rasterpunkte dieser beiden Dimensionen zeigt der Leitfaden dann die betroffenen Prozesse, die möglichen technischen und organisatorischen Maßnahmen und gibt Hinweise auf Normen und Regeln.

1 Einleitung

Das Thema Sicherheit im Umfeld von IT-Lösungen steht im Fokus der öffentlichen Diskussion und stellt damit nicht nur IT-Spezialisten vor neue Herausforderungen. Virenattacken, Ausspähversuche von Daten, die unrechtmäßige Verwendung von elektronischen Identitäten und ähnliche Vorgänge sensibilisieren und verunsichern die Kunden wie Anbieter von IT zunehmend.

Gerade bei einem Application Service Providing-Dienst (ASP) ist das Thema Sicherheit ein wichtiger Aspekt beim Design eines Angebots aber auch bei der Auswahl eines geeigneten Anbieters. Sicherheitsrelevante Vorfälle im ASP-Umfeld sind nicht nur für den tatsächlichen oder vermeintlichen Verantwortlichen unangenehm. In vielen Fällen muss davon ausgegangen werden, dass das Vertrauen auch in den nicht beteiligten Partner erschüttert wird und somit das Image langfristig Schaden nehmen kann.

So führen etwa Vorfälle aufgrund von Nachlässigkeiten beim Kunden trotzdem zu einem Vertrauensverlust für den Anbieter, teilweise für das ASP-Modell generell. Und auch bei klaren Versäumnissen des Anbieters erschüttern gelungene Angriffe auch den guten Ruf der ASP-Kunden.

Letztlich sorgt der bewusste und sensible Umgang mit Daten und Dienstleistungen im Zusammenspiel zwischen dem Kunden und dem Anbieter der Lösung für Sicherheit. Eine Reihe von Schnittstellen und eine Vielzahl von Komponenten, die in den unterschiedlichen Verantwortungsbereichen liegen, sind hierbei zu berücksichtigen.

Der Arbeitskreis ASP des BITKOM hat deshalb die hier beschriebene Checkliste zum Thema Sicherheit erarbeitet, um beiden Partnern einer ASP-Dienstleistung (Kunde und Anbieter) die Möglichkeit zu geben, strukturiert das Thema Sicherheit im eigenen Verantwortungsbereich zu analysieren und kritische Sicherheitsaspekte im Verantwortungsbereich des potenziellen Partners zu hinterfragen. Allgemeine und ergänzende Hinweise zur IT-Sicherheit sind im BITKOM-Leitfaden „Sicherheit in Unternehmen und in Netzen“ des AK Sicherheit von Unternehmensnetzen zu finden.

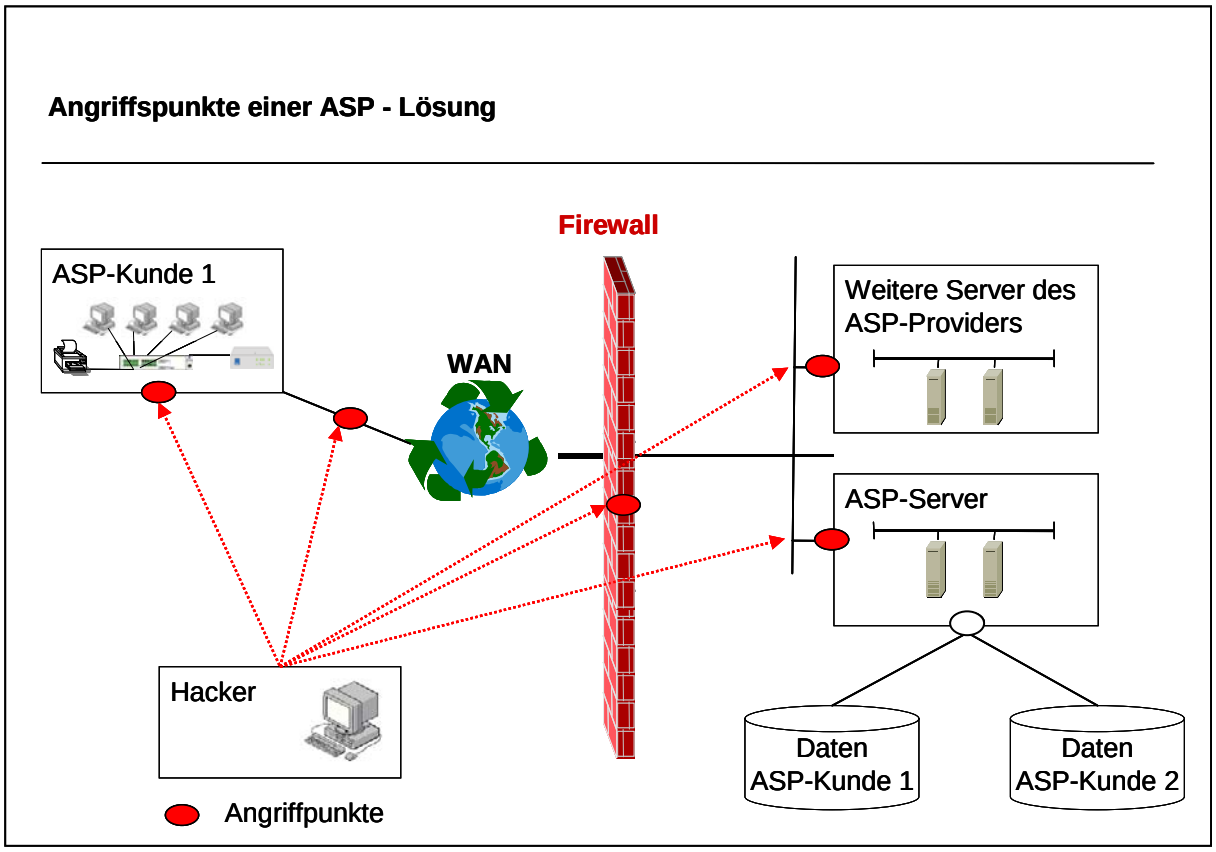
Die Checkliste adressiert sowohl Fragen der Virensicherheit als auch Fragen der Datensicherheit und des Datenschutzes. Neben Maßnahmen gegen mögliche Angriffsszenarien durch Viren, Trojaner usw. stehen die Aspekte zur Sicherung der Datenvertraulichkeit und der Datenintegrität ebenso im Fokus wie Fragen zur Analyse von Schwachstellen bei der Abwehr von Zerstörungsversuchen. Weitere Qualitätsmerkmale von ASP-Diensten bleiben in dieser Liste hingegen unberücksichtigt, darunter z.B. die „Quality of Service“, also die Verfügbarkeit und Ausfallsicherheit.

Generell ist bei dem Querschnittsthema Sicherheit, die zu Grunde liegende Architektur in ihrer Gesamtheit zu betrachten. Die adressierten Fragen, sollen daher eine Orientierungshilfe zu den einzelnen Objekten und den unterschiedlichen Dimensionen einer Architektur geben. Auf Basis dieser Fragen, die als eine Leitlinie zur Analyse der sicherheitsrelevanten Fragestellungen, anzusehen sind, soll die Gesamtbewertung durchgeführt werden. Die Bewertung der Fragen und Anmerkungen obliegt somit den Beteiligten des konkreten ASP-Einsatzes, da insbesondere die Relevanz möglicher Sicherheitsmaßnahmen und die Notwendigkeit zur Erreichung bestimmter Sicherheitslevels nicht allgemeingültig vorgegeben werden können.

Die Fragen der Checkliste sind dabei in verschiedene Kategorien eingeteilt. Neben der generellen Unterscheidung des Verantwortungsbereichs (Kunde, Anbieter) erfolgt die Gliederung

nach den physischen Objekten, die in einer ASP-Lösung eine wesentliche Rolle spielen. Dies sind Endgeräte, Server, Netze, sonstige Infrastruktur und die Daten.

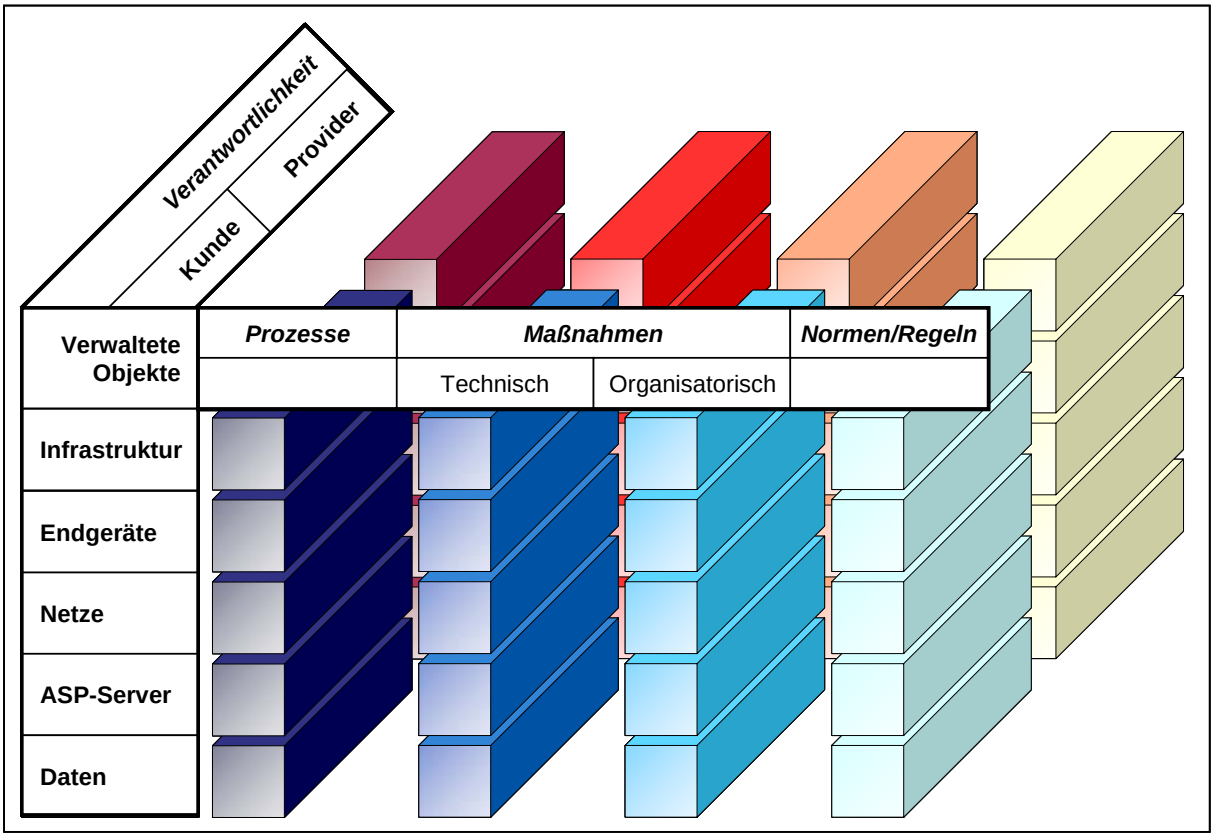
Die folgende Abbildung zeigt in diesem Zusammenhang typische Angriffspunkte bei einer ASP-Lösung:



Den Gliederungselementen **Objekte** und **Verantwortlichkeit** sind dann noch die verschiedenen sicherheitsrelevanten Bereiche die auf dieses Objekte wirken, zugeordnet. Dies sind **Prozesse, Maßnahmen (technisch/organisatorisch), Regeln/Normen**.

2 Übersicht

2.1 Kategorisierung des Leitfadens



Innerhalb jedes Blockes (siehe Abbildung S. 6), werden die entsprechenden Fragen für die jeweiligen Maßnahmen in Bezug auf ein Objekt und auf den jeweiligen Verantwortungsbereich zusammengefasst.

Eine Erfüllung der notwendigen Sicherheitsanforderungen ist nur möglich, wenn die getroffenen technischen und organisatorischen Maßnahmen in ihrer Gesamtheit einen ausreichenden Schutz bieten. Art und Umfang der notwendigen Sicherungsmaßnahmen richten sich nach der Sensibilität der verarbeiteten Daten und nach der jeweiligen technischen Anbindung des Kunden an den Provider.

2.2 Erläuterung der Achsen

Entlang der X-Achse, werden die empfohlenen **Prozesse, Maßnahmen** und vorhandener **Normen und Regeln** dargestellt.

Entlang der Y-Achse, die Unterscheidung der **„Verwaltete Objekte“**:

- Infrastruktur: Dieses Objekt steht stellvertretend für eine unternehmensweite Sicht und jegliche Art von Infrastruktur, die nicht Netz ist, d.h. Gebäude, Klimaanlagen, Stromversorgung, etc.
- Endgeräte: Die Arbeitsstationen, mit denen der Kunde den ASP-Dienst nutzt
- Netze: WAN: Anbindung des Kunden an den ASP-Provider LAN: Netzwerk der Clients und der ASP-Server
- ASP-Server: Die Server, mit denen der ASP-Dienst angeboten wird
- Daten: Produktive Kundendaten

Entlang der Z-Achse, die Unterscheidung der **„Verantwortungsbereiche“**:

- Kunde Fragen die sich der Kunde stellen sollte
- Provider Fragen die sich der ASP-Provider stellen sollte

3 Verantwortungsbereich „Kunde“

Sobald ein Unternehmen eine Internetverbindung herstellt, sind umfangreiche Sicherungsmassnahmen dringend erforderlich, um die Gefahren durch böswillige Angriffe oder eine fahrlässiger Nutzung zu minimieren. Die meisten der für die Nutzung von ASP-Diensten erforderlichen Sicherheitsvorkehrungen sind daher bereits aus anderen Gründen umgesetzt worden. Die nachfolgende Auflistung dient daher insbesondere zur Kontrolle der Vollständigkeit der bereits getroffenen Maßnahmen: Der Kunde muss die Verantwortung für die ihm zugänglichen Objekte der von ihm lizensierten ASP-Dienste tragen. Daher liegen insbesondere die nachfolgenden Objekte in seinem Verantwortungsbereich (siehe Tabelle). Zudem hat der Kunde zu prüfen, ob der Provider seiner Sorgfaltspflicht bei der Einhaltung von Sicherheitsbestimmungen (siehe Tabelle S. 16) nachkommt.

In der nachfolgenden Tabelle sind die Aspekte zusammengestellt, die eine grundlegende Bedeutung besitzen, um unternehmensweite Sicherheitsprozesse sicherzustellen. Diese Zusammenstellung richtet sich insbesondere an die IT-Entscheider in den Unternehmen. Administratoren und Projektgruppen, die in die ASP-Einführung eingebunden sind, finden eine detailliertere Darstellung in der Tabelle ab Seite 11.

Verwaltete Objekte	**Prozesse**	**Maßnahmen**		**Normen/ Regeln**
		Technisch	Organisatorisch	
Unternehmen und Infrastruktur	■ unternehmensweite Sicherheitsprozesse		**Allgemeine Sicherheitsrichtlinien** ■ Gibt es Sicherheitsrichtlinien im Unternehmen? ■ Sind die Sicherheitsprozesse detailliert beschrieben?	ITIL, BDSG, IT-Grundschutzhandbuch, COBIT, etc.
Endgeräte		■ Wird der physische Zugang von Unbefugten zu den Endgeräten verhindert? **Virenprävention** ■ Wird überwacht, ob am Endgerät ein aktueller Virenscanner eingesetzt wird? ■ Werden regelmäßige Virenscans überwacht? **Schutz des Endgerätes gegen Angriffe aus dem Internet** ■ Sind die anonymen Anmeldemöglichkeiten (guest account, etc.) an Ihren Systemen deaktiviert worden? ■ Sind die Internet-Sicherheitseinstellungen restriktiv genug (kein Download von Spielen, Plug-Ins oder ActiveXControls, kein 'Chatten' und keine Onlinespiele am Arbeitsplatz, etc.)?	**Identitätsmanagement** ■ Gibt es ein persönliches Passwort für jeden Benutzer und werden diese einer bestimmten Benutzergruppe mit vordefinierten Zugriffsrechten zugeteilt?	

Verwaltete Objekte	Prozesse	Maßnahmen		Normen/ Regeln
		Technisch	Organisatorisch	
Netze		**Sicherheit im LAN** ■ Werden Firewalls eingesetzt? ■ Gibt es eine mehrstufige heterogene Firewallarchitektur mit Paketfiltern und Application Gateways? **Sicherheit im WAN** ■ Wie ist die Kommunikation zum Provider gesichert? ■ Ist der Zugang zum Provider nur über eine gesicherte und verschlüsselte VPN Anbindung möglich?		

Der Schutz vor systematischen Angriffen ist so gut wie das schwächste Glied in der Kette. Daher muss ein umfassender Schutz durch viele Detailmaßnahmen abgesichert werden. Dies bedeutet, dass durch die zuständigen Fachkräfte insbesondere auch die folgenden Aspekte überprüft werden müssen, um eine reibungslose Nutzung von ASP-Diensten zu ermöglichen.

Verwaltete Objekte	**Prozesse**	**Maßnahmen**		**Normen/ Regeln**
		Technisch	Organisatorisch	
Unternehmen und Infrastruktur	■ Arbeitsprozesse ■ unternehmensweite Sicherheitsprozesse		**Allgemeine Sicherheitsrichtlinien** ■ Gibt es Sicherheitsrichtlinien im Unternehmen? ■ Sind diese in die Arbeitsprozesse integriert und mit anderen Unternehmensrichtlinien abgestimmt? ■ Wie lauten die Ziele und Prinzipien der Sicherheitsrichtlinien? ■ Wie ist ihre Bedeutung in der Unternehmenskultur? ■ Sind die Sicherheitsprozesse detailliert beschrieben? ■ Sind dabei alle notwendigen Funktionen und Verantwortlichkeiten berücksichtigt worden? ■ Sind die Verantwortlichkeiten der Mitarbeiter klar definiert und wissen die Mitarbeiter darüber Bescheid? ■ Gibt es eine Vertreterregelung/ Eskalationsmodell für Mitarbeiter und Verantwortliche? ■ Wie wird im Fall von Störungen der Sicherheit vorgegangen (Notfallplan)? **Sicherheitsrichtlinien für Mitarbeiter** ■ Gibt es Geheimhaltungsvereinbarungen? ■ Werden ausreichende Schulungen für die Mitarbeiter angeboten? ■ Gibt es allgemein bekannte Disziplinarmaßnahmen bei Missachtung der Richtlinien oder Missbrauch? ■ Wird den Mitarbeitern die	ITIL, BDSG, IT-Grundschutzhandbuch, COBIT, etc.

Verwaltete Objekte	Prozesse	Maßnahmen		Normen/ Regeln
		Technisch	Organisatorisch	
			Bedeutung von Sicherheitsmaßnahmen deutlich gemacht?	
Endgeräte	■ Benutzerverwaltung ■ System-Management ■ Fehler- und Störungsmanagement	**Automatisierte Regelung des Zugriffsmanagements** ■ Wird der physische Zugang von Unbefugten zu den Endgeräten verhindert? ■ Werden die Endgeräte ausschließlich in der gleichen Sicherheitszonen eingesetzt (z.B. beim Notebook: Anmeldung im Unternehmens-LAN und Zuhause beim privaten Internetprovider)? ■ Sind die Datenspeicher gesichert und verschlüsselt (z.B. Zugriffsicherung im Falle eines PC-Diebstahls)? ■ Gibt es für Betriebssysteme, Anwendungsprogramme und Dateien differenzierte Zugriffsberechtigungen? ■ Gibt es Passwort-Richtlinien und werden diese durch automatische Policies durchgesetzt? **Virenprävention** ■ Wird überwacht, ob am Endgerät ein aktueller Virenscanner eingesetzt wird? ■ Werden regelmäßige Virenscans überwacht? **Schutz des Endgerätes gegen Angriffe aus dem Internet** ■ Wird ein Internet-Zugang auf den Engeräten benötigt? ■ Werden lokale Firewalls eingesetzt? ■ Sind alle nicht erforderlichen Dienste und Programme so weit wie möglich deaktiviert? ■ Sind die anonymen Anmeldemöglichkeiten (guest account, etc.) an Ihren Systemen deaktiviert worden? ■ Werden die Systeme vom Internet getrennt, wenn ein	■ Wurde festgelegt, dass die ASP-Zugangsdaten nicht auf den Endgeräten hinterlegt werden dürfen? **Identitätsmanagement** ■ Gibt es ein persönliches Passwort für jeden Benutzer und werden diese einer bestimmten Benutzergruppe mit vordefinierten Zugriffsrechten zugeteilt? ■ Werden die Benutzer- und Passwortlisten bei Personalwechsel immer aktualisiert? ■ Werden alle Passwörter in einem definiertem Abstand gewechselt und entsprechen diese bestimmten Passwortrichtlinien? ■ Wird vermieden, dass Passwörter unverschlüsselt auf der Festplatte gespeichert werden? ■ Sind die Prozesse zur Festlegung und Erneuerung von Passwörtern formalisiert und automatisiert? **Virenprävention** ■ Gibt es eine Richtlinie, die sicherstellt, dass die Mitarbeiter zyklisch Ihren Viren-Scanner aktualisieren und einen Virenscan durchführen? ■ Gibt es Disziplinarmaßnahmen (z.B. Zugriff auf Netzwerkressourcen verweigern), falls der Viren-Scanner nicht aktuell ist bzw. kein Virenscan durchgeführt wurde? **Wartung der Systeme** ■ Gibt es intern einen Verantwortlichen, der sich um die Wartung aller Endgerät-	BSI, ITIL, BDSG, COBIT, etc.

Verwaltete Objekte	Prozesse	Maßnahmen		Normen/ Regeln
		Technisch	Organisatorisch	
		ASP-Zugang aufgebaut wird? ■ Sind die Internet-Sicherheitseinstellungen restriktiv genug (kein Download von: Spielen, Plug-Ins oder ActiveXControls, kein 'Chatten' und keine Onlinespiele am Arbeitsplatz, etc.)?	Systeme kümmert? ■ Werden die Systeme regelmäßig aktualisiert (Service Packs, Hotfixes, Security-Patches, etc.)? ■ Werden nur Softwareprodukte verwendet, die vom Hersteller noch unterstützt und weiterentwickelt wird? (Ältere Versionen erfüllen heutige Sicherheitsanforderungen meistens nur bedingt.) ■ Wird überflüssige Soft- und Hardware von den Endgerät-Systemen entfernt und wird sichergestellt, dass die Mitarbeiter keine private Soft- und Hardware installieren können? ■ Werden die Sicherheitskomponenten der Endgerät-Systeme regelmäßig gewartet? ■ Wird vermieden, dass Zugangsdaten des ASP-Zugangs elektronisch hinterlegt werden? **Schutz der Endgeräte gegen Angriffe aus dem Internet** ■ Wird ein Internet-Zugang auf den Endgeräten benötigt? ■ Wurden betriebsinterne Regeln aufgestellt, die den Umgang mit dem Internet regeln (kein Download von: Spielen, Plug-Ins oder ActiveXControls, kein 'Chatten' und keine Onlinespiele am Arbeitsplatz, etc.)? ■ Wurde den Mitarbeitern vermittelt, dass alle e-Mails oder Programme, die über das Internet empfangen werden, generell als unsicher zu betrachten sind?	
Netze	■ Fehler- und Changemanagement	■ Wird der physische Zugang von Unbefugten zu den Netzwerk-Komponenten verhindert?	■ Gibt es einen internen Verantwortlichen, der sich um die Sicherheit im Netzwerk kümmert?	BSI

Verwaltete Objekte	Prozesse	Maßnahmen		Normen/ Regeln
		Technisch	Organisatorisch	
	■ Monitoring	**Sicherheit im LAN** ■ Werden Firewalls eingesetzt? ■ Gibt es eine mehrstufige heterogene Firewallarchitektur mit Paketfiltern und Application Gateways? ■ Wird eine Mail-Security Gateway eingesetzt? ■ Welche Technologie wird zum Erkennen und zur Überwachung von Eindringversuchen eingesetzt? ■ Wird die Netzinfrastruktur regelmäßig durch z.B. Penetrationen auf Sicherheitslücken untersucht? ■ Ist der externe Zugang nur über eine gesicherte und verschlüsselte VPN Anbindungen möglich? **Sicherheit im WAN** ■ Wie ist die Kommunikation zum Provider gesichert? ■ Ist der Zugang zum Provider nur über eine gesicherte und verschlüsselte VPN Anbindung möglich? ■ Wie wird sichergestellt, dass vom Endgerät der richtige Server angesprochen wird?	■ Gibt es eine Vertreterregelung/ Eskalationsmodell für Verantwortliche? ■ Wie wird sichergestellt, dass weder Passwörter noch Daten mitgeschnitten werden?	
Verbindung zum ASP-Server			■ Muss es eine direkte Schnittstelle zu den ASP-Servern geben (sog. Client-Drive-Mapping)? ■ Kann der Anwender Programme oder Skripte auf den Endgeräten installieren und diese dort ausführen?	
Daten	■ Datenträgerentsorgung		■ Werden alle Datenträger datenschutzgerecht entsorgt?	

4 Verantwortungsbereich „Provider“

Der Provider hat den Kunden auf seinen Verantwortungsbereich hinzuweisen (siehe Tabelle S. 9) und zudem insbesondere für die nachfolgenden Objekte die Verantwortung zu übernehmen:

Verwaltete Objekte	**Prozesse**	**Maßnahmen**		**Normen/ Regeln**
		Technische	Organisatorische	
Unternehmen und Infrastruktur	■ Arbeitsprozesse ■ unternehmensweite Sicherheitsprozesse	**Sicherung von Grundstück und Gebäude** ■ Sind die Anforderung an Raum und Gebäude (Innenausbau aus Massivwänden, sicher gegen Wassereinbruch, einbruchsichere Fenster, Türen, Licht- und Lüftungsschächte) in aureichendem Maß erfüllt? ■ Sind automatische Zutrittskontrollen vorhanden? ■ Werden alle Zutrittsvorgänge dokumentiert? ■ Ist das Firmengelände in Sicherheitszonen mit abgestuften Zutrittsberechtigungen eingeteilt? ■ Videoüberwachung (Raum- und Zugangsüberwachung) vorhanden? ■ Ist eine Einbruchmeldeanlage gemäß der Vorgaben des VdS und des BHE mit Wachdienstaufschaltung vorhanden? ■ Wie wird mit Besuchern auf dem Firmengelände umgegangen, z.B. Zutritt nur in Begleitung berechtigter Personen? ■ Wie werden Gebäude selbst gesichert? ■ Sind Wasser- und Brandmelder vorhanden und werden Störungsfälle an verantwortliche Stellen weitergemeldet?	**Allgemeine Sicherheitsrichtlinien** ■ Gibt es Sicherheitsrichtlinien im Unternehmen? ■ Sind diese in die Arbeitsprozesse integriert und mit anderen Unternehmensrichtlinien abgestimmt? ■ Wie lauten die Ziele und Prinzipien der Sicherheitsrichtlinien? ■ Wie ist ihre Bedeutung in der Unternehmenskultur? ■ Sind die Sicherheitsprozesse detailliert beschrieben? ■ Sind dabei alle notwendigen Funktionen und Verantwortlichkeiten berücksichtigt worden? ■ Sind die Verantwortlichkeiten der Mitarbeiter klar definiert und wissen die Mitarbeiter darüber Bescheid? ■ Gibt es eine Vertreterregelung/ Eskalationsmodell für Mitarbeiter und Verantwortliche? ■ Wie wird im Fall von Störungen der Sicherheit vorgegangen? (Notfallplan?) ■ Wie wird die Implementierung und Einhaltung der Sicherheitsrichtlinien sichergestellt? ■ Werden Sicherheits-Audits am System durchgeführt? ■ Wie wird der Missbrauch von IT-Ressourcen festgestellt und welche Konsequenzen entstehen daraus? ■ Werden die Sicherheitsaspekte anderer EDP Audits	ITIL, BDSG, IT-Grundschutzhandbuch, ISO, COBIT, etc.

Verwaltete Objekte	Prozesse	Maßnahmen		Normen/ Regeln
		Technische	Organisatorische	
			übernommen? **Sicherheitsrichtlinien für Mitarbeiter** ■ Gibt es Geheimhaltungsvereinbarungen? ■ Werden ausreichende Schulungen für die Mitarbeiter angeboten? ■ Gibt es allgemein bekannte Disziplinarmaßnahmen bei Missachtung der Richtlinien oder Missbrauch? ■ Wird den Mitarbeitern die Bedeutung von Sicherheitsmaßnahmen deutlich gemacht?	

Endgeräte (des Kunden)		■ Wird die Kommunikation über evtl. vorhandene Schnittstellen zum Endgerät überwacht?
		■ Werden Mechanismen aus dem Bereich des Endgeräte-Managements eingesetzt?
		  ■ Zur Aktualisierung der Endgeräte-Konfiguration?
		  ■ Zur Aktualisierung des Viren-Scanners
		  ■ Zur Überwachung des Endgeräte-LANs
		■ Gibt es für Betriebssysteme, Anwendungsprogramme und Dateien differenzierte Zugriffsberechtigungen?
		■ Liegt ein softwareseitiger Ausschluss vor (Mandantentrennung)?
			■ Muss es eine direkte Schnittstellen zu den Engerät-Systemen geben (Client-Drive-Mapping)?
			■ Kann der Anwender Programme oder Skripte auf den Engeräten installieren und diese dort ausführen?
			■ Ist der Kunde über vorhandene Richtlinien informiert (z.B. kein lokaler Internet Zugang auf den Endgeräten, aktueller Virenscanner, etc.)?
			■ Wurde festgelegt, dass der Kunde die ASP-Zugangsdaten nicht auf den Endgeräten hinterlegt darf?	

Endgeräte (des Providers)	■ Benutzerverwaltung ■ System-Management ■ Fehler – und Störungsmanagement	**Automatisierte Regelung des Zugriffsmanagements** ■ Wird der physische Zugang von Unbefugten zu den Endgeräten verhindert? ■ Wird das Endgerät ausschließlich in der gleichen Sicherheitszonen eingesetzt (z. B. beim Notebook: Anmeldung im Unternehmens-LAN und Zuhause beim privaten Internetprovider) ■ Sind die Datenspeicher gesi-	**Identitätsmanagement** ■ Gibt es ein persönliches Passwort für jeden Benutzer und werden diese einer bestimmten Benutzergruppe mit vordefinierten Zugriffsrechten zugeteilt? ■ Werden die Benutzer- und Passwortlisten bei Personalwechsel immer aktualisiert? ■ Werden alle Passwörter in einem definiertem Abstand	BSI, ITIL, BDSG, COBIT, etc.

Verwaltete Objekte	Prozesse	Maßnahmen		Normen/ Regeln
		Technische	Organisatorische	
		chert und verschlüsselt (z.B.: Zugriffsicherung im Falle eines PC-Diebstahls)? ■ Gibt es Passwort-Richtlinien und werden diese durch automatische Policies durchgesetzt? **Virenprävention** ■ Wird überwacht, ob am Endgerät ein aktueller Virenscanner eingesetzt wird? ■ Werden regelmäßige Virenscans überwacht? **Schutz der Engeräte gegen Angriffe aus dem Internet** ■ Wird ein Internet-Zugang auf den Engeräten benötigt? ■ Werden lokale Firewalls eingesetzt? ■ Ist das Engerät gehärtet (sind alle nicht erforderlichen Dienste und Programme so weit wie möglich deaktiviert)? ■ Können anonyme Anmeldemöglichkeiten (guest account, etc.) an Ihren Systemen deaktiviert werden? ■ Werden die Systeme vom Internet getrennt, wenn ein ASP-Zugang aufgebaut wird? ■ Sind die Internet-Sicherheitseinstellungen restriktiv genug (kein Download von: Spielen, Plug-Ins oder ActiveXControls, kein 'Chatten' und keine Onlinespiele am Arbeitsplatz, etc.)?	gewechselt und entsprechen diese bestimmten Passwortrichtlinien? ■ Wird vermieden, dass Passwörter auf der Festplatte gespeichert werden? ■ Sind die Prozesse zur Festlegung und Erneuerung von Passwörtern formalisiert und automatisiert? **Virenprävention** ■ Gibt es eine Richtlinie, die sicherstellt, dass die Mitarbeiter zyklisch Ihren Virenscanner aktualisieren und einen Virenscan durchführen? ■ Gibt es Disziplinarmaßnahmen (z.B. verweigern des Zugriffs auf bestimmte Netzwerkressourcen), falls der Virenscanner nicht aktuell ist bzw. kein Virenscan durchgeführt wurde? **Wartung der Systeme** ■ Gibt es intern einen Verantwortlichen, der sich um die Wartung aller Engerät-Systeme kümmert? ■ Werden die Systeme regelmäßig aktualisiert (Service Packs, Hotfixes, Security-Patches, etc.)? ■ Werden nur Softwareprodukte verwendet, die vom Hersteller noch unterstützt und weiterentwickelt wird? (Ältere Versionen erfüllen heutige Sicherheitsanforderungen meistens nur bedingt) ■ Wird überflüssige Soft- und Hardware von den Endgerät-Systemen entfernt und wird sichergestellt, dass die Mitarbeiter keine private Soft- und Hardware installieren können? ■ Werden die Sicherheits-	

Verwaltete Objekte	Prozesse	Maßnahmen		Normen/ Regeln
		Technische	Organisatorische	
			komponenten der Endgerät-Systeme regelmäßig gewartet? ■ Wird vermieden, dass Zugangsdaten des ASP-Zugangs elektronisch hinterlegt werden? **Schutz der Endgeräte gegen Angriffe aus dem Internet** ■ Wird ein Internet-Zugang auf den Endgeräten benötigt? ■ Wurden betriebsinterne Regeln aufgestellt, die den Umgang mit dem Internet regeln (kein Download von: Spielen, Plug-Ins oder ActiveXControls, kein 'Chatten' und keine Onlinespiele am Arbeitsplatz, etc.)? ■ Wurde den Mitarbeitern vermittelt, dass alle e-Mails oder Programme, die über das Internet empfangen werden, generell als unsicher zu betrachten sind?	
Netze	■ Fehler- und Changemanagement ■ Netzwerk-Monitoring ■ Change-Management	■ Wird der physische Zugang von Unbefugten zu den Netzwerk-Komponenten verhindert? **Sicherheit im ServerLAN** ■ Werden Firewalls eingesetzt? ■ Gibt es eine mehrstufige heterogene Firewallarchitektur? ■ Welche Technologie wird zur Erkennung und zur Überwachung von Eindringversuchen eingesetzt? ■ Kommen Web-Services zum Einsatz? ■ Ist die Firewall darauf abgestimmt? ■ Wird ein Content–Filter eingesetzt? ■ Werden alle Anmeldeversuche überwacht und dokumentiert (Accounting)?	■ Gibt es einen internen Verantwortlichen, der sich um die Sicherheit im Netzwerk kümmert? ■ Gibt es eine Vertreterregelung /Eskalationsmodell Verantwortliche? ■ Wie wird sichergestellt, dass weder Passwörter noch Daten mitgeschnitten werden? ■ Wie werden diese Maßnahmen überwacht? ■ Gibt es eine Bereitschaftsdienst-Regelung, die jeder Zeit erforderliche Maßnahmen auf sicherheitskritische Vorfälle sicherstellt? ■ Wie wird sichergestellt, dass nur autorisierte Web-Services zum Einsatz kommen? ■ Kann sichergestellt werden, dass Sperrlisten zeitnah	

Verwaltete Objekte	Prozesse	Maßnahmen		Normen/ Regeln
		Technische	Organisatorische	
		■ Können anonyme Anmeldemöglichkeiten (guest account, etc.) an allen Server-Systemen deaktiviert werden? ■ Wird die Netzinfrastruktur regelmäßig durch z.B. Penetrationen auf Sicherheitslücken untersucht? ■ Werden es neben den ASP-Servern noch andere Server betrieben? ■ Sind die Server untereinander erreichbar? ■ Sind die Zugangssicherungsmaßnahmen der anderen Server gleich hoch? **Sicherheit im WAN** ■ Wie ist die Kommunikation zum Kunden gesichert? ■ Haben die eingesetzten Verfahren ein Zertifikat für die Einhaltung von IPSEC? ■ Ist der Zugang zum Kunden nur über eine gesicherte und verschlüsselte Anbindung möglich? ■ Wie wird sichergestellt, dass vom Endgerät der richtige Server angesprochen wird?	(entsprechend der Unternehmenspolicy) verteilt werden?	
ASP-Server	■ Benutzerverwaltung ■ Fehlermanagement ■ System-Management ■ Netzwerk-Monitoring ■ Change-Management	■ Wird der physische Zugang von Unbefugten zu den ASP-Server-Systemen verhindert? ■ Sind Produktiv- und Test-Systeme voneinander getrennt? ■ Wie wird mit Security-Patches zu den beteiligten Softwarekomponenten (Anwendung, Middleware, Betriebssystem) umgegangen? **Authentifizierung am Server** ■ Werden Passwort-Richtlinien durch automatische Policies durchgesetzt? ■ Werden regelmäßig Tests gegen alle Accounts durchgeführt, die die Güte der	**Authentifizierung am Server** ■ Gibt es Richtlinien zur Bildung von Passwörtern und werden diese überprüft? ■ Gibt es neben der Wissenskomponenten User-ID und Passwort noch Besitzkomponenten, z.B. Smart-Card oder Security-Token, die für den Zugang notwendig sind? ■ Wie ist die Verwaltung geregelt? **Wartung der Server Systeme** ■ Gibt es intern einen Verantwortlichen, der sich um die Wartung der Systeme kümmert?	

Verwaltete Objekte	Prozesse	Maßnahmen		Normen/ Regeln
		Technische	Organisatorische	
		Passwörter checken (z. B. Passwortcracker)? **Virenprävention** ■ Wird überwacht, ob auf den Servern Systemen ein aktueller Virenscanner eingesetzt wird? ■ Werden regelmäßige Virenscans automatisch durchgeführt? **Schutz des Server-Systems gegen Angriffe aus dem Internet** ■ Wird ein Internet-Zugang des Server-Systems benötigt? ■ Werden Firewalls eingesetzt? ■ Können anonyme Anmeldemöglichkeiten (guest account, etc.) an den Systemen deaktiviert werden? ■ Sind die Internet-Sicherheitseinstellungen für die Kunden restriktiv genug (kein Download von: Spielen, Plug-Ins oder ActiveX-Controls, kein 'Chatten' und keine Onlinespiele am Arbeitsplatz, etc.)? ■ Erfolgt der Zugriff auf das ASP-System über eine gesichterte Verbindung (Datenverschlüsselung z. B. über IPSEC oder SSL)? ■ Sind die ASP-Server gehärtet (alle nicht erforderlichen Dienste werden deaktiviert)? ■ Wird SSL-Verschlüsselung (https) angeboten, wurde das Zertifikat von einer vertrauenswürdigen CA-Stelle (Trustcenter) ausgestellt? ■ Gibt es ein Mehrzonen-Sicherheitskonzept, d.h.: steht der Server mit Nutzerdaten und kritischen Informationen (DB-Server) in einer höheren Sicherheitszone, als das System, auf welches vom Engerät zugegriffen wird	■ Werden die Systeme regelmäßig aktualisiert (Service Packs, Hotfixes, Security-Patches, etc.)? ■ Werden nur Softwareprodukte verwendet, die vom Hersteller noch unterstützt und weiterentwickelt wird? (Ältere Versionen erfüllen heutige Sicherheitsanforderungen meistens nur bedingt) ■ Sind Audits durch Externe vorgesehen?	

Verwaltete Objekte	Prozesse	Maßnahmen		Normen/ Regeln
		Technische	Organisatorische	
		(z.B. Applikationsserver/ Webserver)? **Verfügbarkeitskontrolle** ■ Gibt es ein Backup-Rechenzentrum? ■ In welchem Status befindet es sich (Hot Stand-by, Warm Stand-by, Cold)? ■ Sind redundante Hotplug-Komponenten aller Spannungsführenden und kühlenden Komponenten vorhanden? ■ Ist eine unterbrechungsfreie Stromversorgung (USV) vorhanden und gewährleistet? ■ Ist das Rechenzentrum klimatisiert? ■ Sind die Systeme permanent überwacht und ist im Störungsfall eine Alarmierung durch Systemmanagement-Software gewährleistet?		
Daten	■ Backup-Management ■ Datenträgerentsorgung ■ Katastrophen-Recovery-Management	■ Sind die Datensicherungen gegen unbefugten Zugriff geschützt? ■ Sind die Ressourcen der einzelnen ASP-Nutzer sicher getrennt? ■ Welche Technik wird zur Datenverschlüsselung verwendet? ■ Systembereiche Raid 1/ Datenbereiche Raid 5? **Backup-Management** ■ Werden Datenträgerarchive und Datensicherungen sicher und getrennt von den Servern aufbewahrt? ■ Wie und von welchen Systemeinheiten werden Backups erstellt (Datensicherungskonzept?) ■ Wie werden die Backups gesichert? ■ Werden Archive-Logfiles gesichert und überwacht?	■ Werden alle Datenträger datenschutzgerecht entsorgt?	

Verwaltete Objekte	Prozesse	Maßnahmen		Normen/ Regeln
		Technische	Organisatorische	
		■ Wird die Qualität der Back-ups regelmäßig überwacht? ■ Gibt es eine Notfallplanung? **Ressourcen-Handling** ■ Hat jeder Anwender nur eigene Ressourcen oder werden Ressourcen, z.B. Datenbanken, gemeinsam genutzt? ■ Wie stellt die ASP-Anwendung bei gemeinsam genutzten Ressourcen sicher, dass hier nicht ASP-Nutzer unbefugt auf andere Daten zugreifen?		

5 Prinzipielle Fragen zur Organisation der Sicherheit (Information Security Organisation)

- Wie sehen die Rahmenbedingungen und die Struktur der Sicherheitsorganisation und des Sicherheitsmanagements aus?
- Wie sind die Verantwortlichkeiten verteilt (Beschreibung so detailliert wie möglich)?
- Wurde ein Ausschuss zur Steuerung der Sicherheitslösungen gebildet (Information Security Steering Committee)?
- Wie werden die Sicherheitslösungen in der Praxis koordiniert?
- Sind alle Prozesse die Zugriffsberechtigungen und die Zugriffsprozesse auf die Systeme gemeinsam besprochen und dokumentiert worden?
- Wurden Experten zu Rate gezogen?
- Wie sieht die Kooperation zwischen Unternehmen und Provider aus? Wie soll die (externe und interne) Kommunikation ablaufen?
- Wie sind die Sicherheitsrichtlinien definiert, wenn Dritte Zugriff auf das System benötigen? Wie wird in Verträgen mit Dritten mit dem Thema Sicherheit umgegangen?

Glossar

ASP:	Application Service Providing
BDSG:	Bundesdatenschutzgesetz
BHE:	Bundesverband der Hersteller und Errichter von Sicherheitssystemen e.V.
BSI:	Bundesamt für Sicherheit in der Informationstechnik
CA:	Conditional Access
DB:	Datenbank
EDP:	Electronic Data Processing
ID:	Identifikation, Benutzererkennung
IPSEC:	Internet Protocol Security Extensions
ISO:	International Standardization Organization
ITIL:	Information Technology Infrastructure Library
LAN:	Local Area Network
SLA:	Service Level Agreement
SSL:	Secure Socket Layer
USV:	Unterbrechungsfreie Stromversorgung
VdS:	Verbandes der deutschen Sachversicherer
VPN:	Virtual Private Network
WAN:	Wide Area Network

Danksagung

Dieser Leitfaden entstand im BITKOM Arbeitskreis „Application Service Providing“ unter Federführung der

DATEV e.G.

Besondere Unterstützung wurde durch folgende BITKOM-Mitglieder und -Partner geleistet:

Deutsche Telekom Network Projects & Services GmbH,
IBM Deutschland GmbH,
Institut für Wirtschaftsinformatik der Humboldt-Universität zu Berlin,
IT advisory group Unternehmensberatung AG,
Lufthansa Systems Group GmbH,
Microsoft Deutschland GmbH,
Reinhardt und Erben GmbH,
SAP Deutschland AG & Co. KG,
Siemens Business Services GmbH & Co. OHG,
Siemens AG,
Tenovis GmbH & Co. KG,
T-Systems International GmbH und
VRG-Vereinigte Rechenzentren GmbH sowie die

BITKOM-Arbeitskreise „Sicherheit“ und „Mittelstand“.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. vertritt mehr als 1.000 Unternehmen, davon 750 Direktmitglieder mit etwa 120 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Geräte-Hersteller, Anbieter von Software, IT-Services, Telekommunikationsdiensten und Content. Der BITKOM setzt sich insbesondere für bessere ordnungsrechtliche Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.
Albrechtstraße 10
10117 Berlin-Mitte

Tel.: 030/27 576 - 0
Fax: 030/27 576 - 400

bitkom@bitkom.org
www.bitkom.org