ASP-Dienstleistungen und Sicherheit

Sind Sie sicher?

Erfahren Sie, wie ASP Ihre IT-Sicherheit erhöhen kann.

AK ASP

Stand: 12. Juli 2005, Version 1.1

Zielgruppe:

Interessenten für ASP-Dienstleistungen mit k(l)einer IT-Abteilung,

→ KMU mit ca. 10-100 Anwender

Anwendung:

Präsentation bei potentiellen Kunden vor Ort, deren Kerngeschäft wenig IT-fokussiert ist.

Integration von Teilen in firmeneigene Präsentationen, um den Nutzen eines hohen Sicherheitsniveaus bei ASP-Dienstleistungen zu adressieren.

Überblick

IT-Sicherheit soll

- die Verfügbarkeit,
- die Vertraulichkeit,
- und die Integrität

Ihrer Daten und IT-Einrichtungen gewährleisten.

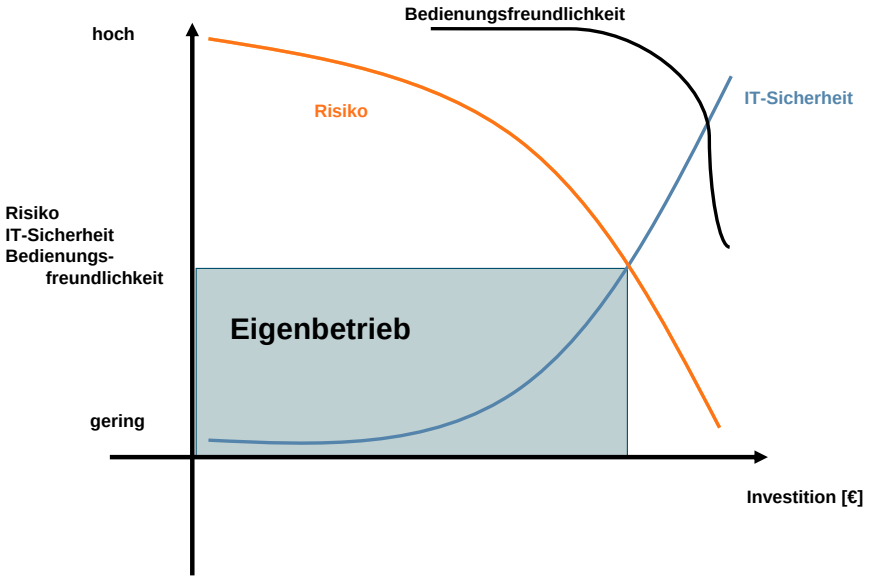
Dies wird dadurch erreicht, dass

- ein unerlaubter Zugang zum Unternehmensnetz verhindert wird,
- ein unerlaubter Zugriff auf Unternehmensdaten unterbunden wird,
- Angriffe auf IT-Einrichtungen abgewendet werden und
- Unternehmensdaten ausreichend gesichert werden.

Sensibilisierung des Themas Sicherheit.

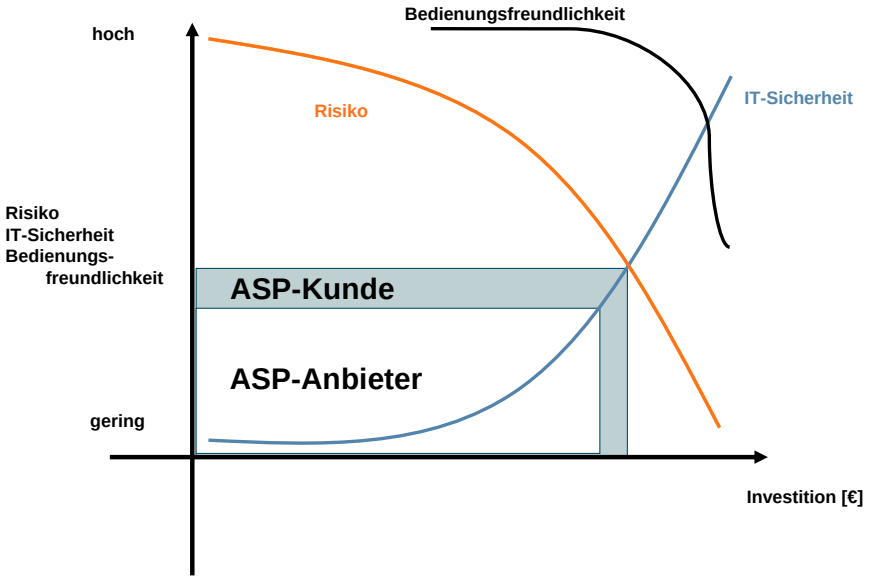
Insbesondere in KMU‘s sind die Maßnahmen zur Datensicherung und zur Sicherheit gegen äussere Angriffe und Einflüsse (z.B. Naturkatastrophen, Unfälle, …) oft unterentwickelt.

Sicherheit erfordert eine hohe Initialinvestition!



Die Folie zeigt die erforderlichen Investitionen bei Unternehmen mit Internetzugang, um alle Zugänge zum IT-System gegen unbefugte Zugriffe abzusichern. Vereinzelte, selektive Maßnahme bieten keinen hinreichenden Schutz.

Sicherheit erfordert eine hohe Initialinvestition!

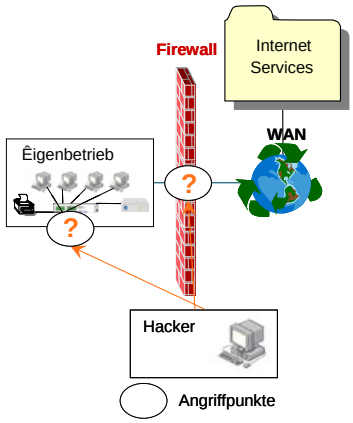


Diese Folie zeigt ebenfalls die erforderlichen Investitionen, um alle Zugänge zum IT-System gegen unbefugte Zugriffe abzusichern. Ein Großteil der erforderlichen Investitionen kann auf den ASP-Anbieter übertragen werden, wodurch die erforderlichen Sicherheitsleistungen des ASP-Kunden deutlich reduziert werden können.

Ihre Aufgaben im Zuge der Internetanbindung

Die „Angriffspunkte“ im Bild unten verdeutlichen die Stellen, an denen ein Angreifer in Ihrer IT-Umgebung tätig werden kann. Für den Schutz dieser Stellen müssen Sie sorgen!

Lesen Sie hierzu die BITKOM Leitfäden „Sicherheit in Unternehmen und in Netzen“.



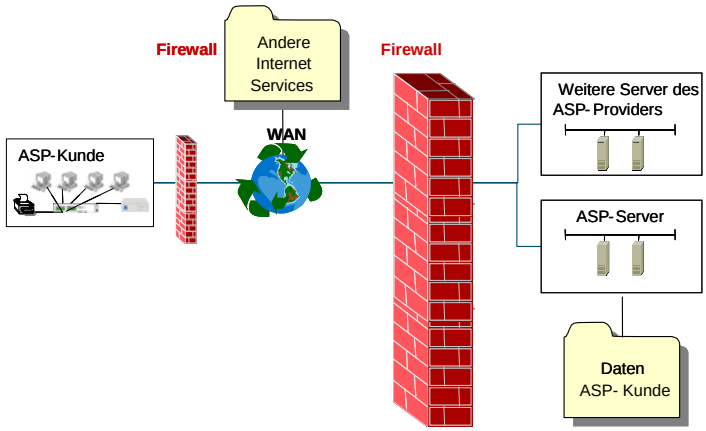
Auf Kundenseite werden die wesentlichen Sicherungsmaßnahmen bereits mit der Internetanbindung erforderlich und sind daher unabhängig von der Nutzung von ASP-Dienstleistungen zu beachten.

Da Sicherheit sehr aufwendig ist, fehlen bei KMU‘s häufig wichtige Basiselemente, wie Firewall, aktuelle Virenscanner, …

Das Besondere an ASP

„Application Service Providing“ (ASP) bedeutet, dass Sie Anwendungen als Dienstleistung eines Dritten beziehen

Das Bild zeigt die Komponenten einer ASP-Lösung: Auf der linken Seite sehen Sie Ihr Unternehmen, auf der rechten Seite das Datenzentrum Ihres ASP-Partners.

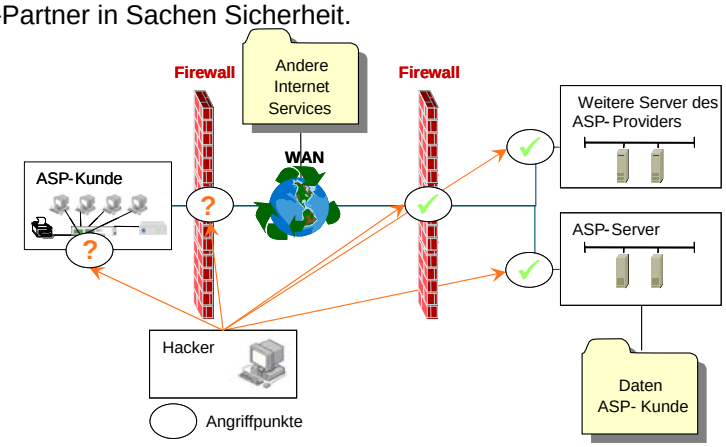


Die ASP-Dienstleistung kommt über eine Datenleitung. Verfügbarkeit und Sicherheit sind die Eckpunkte des Servicelevels.

Wichtige Daten und Anwendungen des KMU‘s können über den ASP-Anbieter gesichert werden.

Die Aufgaben Ihres ASP-Partners

Die drei „Angriffspunkte“ im Bild unten rechts verdeutlichen die Stellen, an denen ein Angreifer in der Umgebung Ihres ASP-Partners eine Manipulation durchführen kann. Ihr ASP-Partner muss für die Sicherheit dieser Stellen sorgen. Auf den folgenden Seiten bekommen Sie eine kleine Anleitung zum Umgang mit Ihrem ASP-Partner in Sachen Sicherheit.

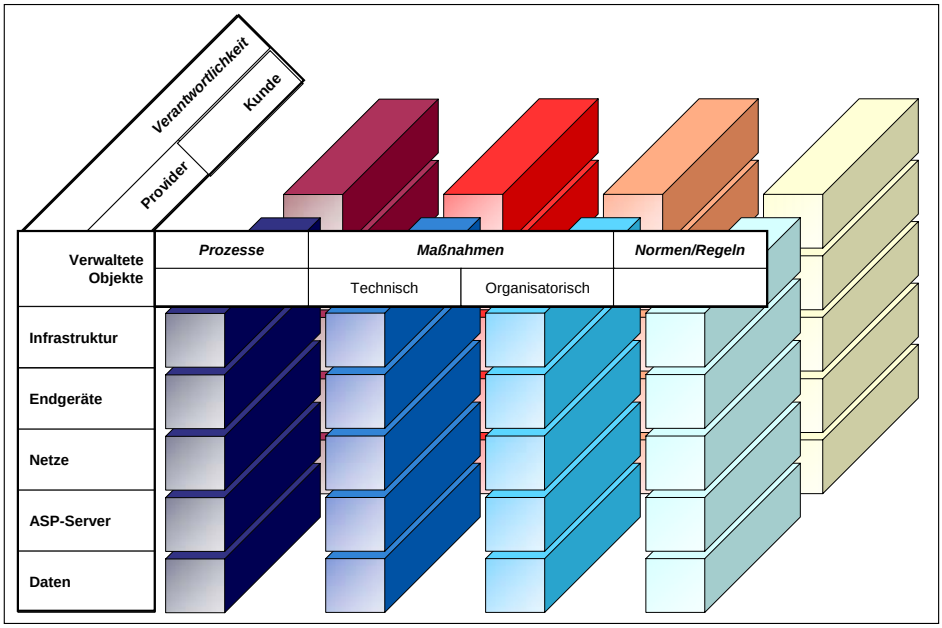


Der ASP-Dienstleister kann die erforderlichen Sicherheitsmaßnahmen durch Skalierungseffekte (Verteilung der Kosten auf viele Kunden) kostengünstig und stets aktuell anbieten.

Der Leitfaden bietet dem Kunden die Möglichkeit, die Sicherheitsmaßnahmen des Anbieters zu hinterfragen und ggf. Schwachstellen aufzudecken. Wichtig ist hierbei die individuelle Einschätzung des erforderlichen Sicherheitsniveaus.

Eine besondere Absicherung ergibt sich durch die Verbindung direkter, geschützter Datenverbindungen, z.B. VPN, https,…

Gliederung des BITKOM Leitfadens „ASP-Sicherheit“



Der Leitfaden strukturiert die Maßnahmen zur Herstellung der benötigten Sicherheit in zwei Dimensionen: Verantwortlichkeiten und verwaltete Objekte.

Der Leitfaden benennt die betroffenen Prozesse, die möglichen technischen und organisatorischen Maßnahmen und die geltenden Normen und Regeln.

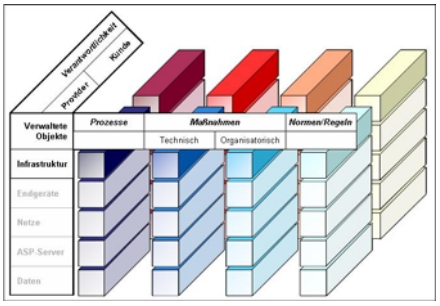
Auf den nachfolgenden Folien werden drei Beispiele gezeigt, bei denen Ihr ASP-Anbieter Sicherheit gewährleisten muß: Infrastruktur (Gebäude, Endgeräte, …), Netze, Daten.

Weitere Details zur Struktur des BITKOM Leitfadens „ASP-Sicherheit“ finden Sie im Anhang.

Sicherheit des Rechenzentrums

Das Rechenzentrum Ihres ASP-Partners muss gegen

- natürliche Schäden (von Feuer, Sturm, Flut usw.) und
- unbefugten Zutritt geschützt werden. Hierzu gehört eine Reihe von Maßnahmen wie zum Beispiel:
  - Wasser- und Brandmelder,
  - automatische Löschsysteme,
  - einbruchsichere Fenster und Türen,
  - Videoüberwachung, etc.



Auch die dazugehörige Prozesse - zum Beispiel, wie auf die Meldung eines Wassereinbruch reagiert wird - sind wichtig.

Details:

BITKOM Leitfaden „ASP Sicherheit“ Seiten 13 und 14

Ein Mangel der Infrastruktur-Sicherung ist „Russisch Roulette“.

Sicherheit des Datennetzes

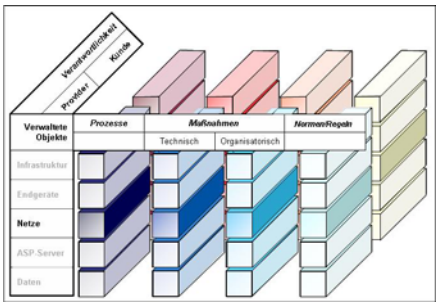
Das Datennetz und die Server Ihres ASP-Partners müssen gegen

- Attacken (Viren, Würmer, Trojaner etc.) aus dem Internet,
- unbefugte Nutzung und
- Abhören durch Dritte

geschützt werden. Einige der Maßnahmen, die hier eingesetzt werden können, sind:

- Eine Firewall,
- Zutritts- und Zugangskontrollen,
- Überwachung von Anmeldeversuche und
- verschlüsselte Übertragung der Daten.

Auch die stetige Überwachung der Netze und Server sowie regelmäßige simulierte Angriffe, um diese Überwachung zu prüfen, gehören hierzu.



Nutzen Sie den BITKOM Leitfaden „ASP Sicherheit“ Seiten 14 bis 18, um die Angaben Ihres ASP-Partners zu bewerten.

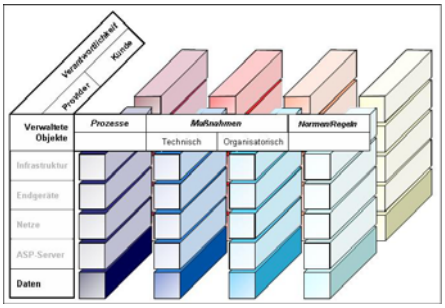
Viren erreichen in weniger als einem Tag 80% Ihrer Gesamtverbreitung. hochfrequente Software-Updates sind daher unumgänglich.

Zugangs-Passwörter gewährleisten nur bei regelmäßiger Änderung, dass nur befugte Mitarbeiter auf das System und die Daten zurückgreifen.

Sicherheit der Daten

Die Daten – Ihre Daten – müssen beim ASP-Partner gegen Verlust und Datenklau geschützt werden. Viele der Maßnahmen, die weiter oben in dieser Kurzanleitung beschrieben wurden, dienen dazu, die Möglichkeiten des Datendiebstahls zu verhindern. Zusätzlich sollte Ihr ASP-Partner insbesondere dafür sorgen, dass

- nicht mehr benötigte Datenträger datenschutzgerecht entsorgt werden,
- es eine strikte Trennung zwischen seinen Mandanten gibt,
- die Daten regelmäßig gesichert werden und
- Sicherungskopien an einem zweiten, sicheren Ort aufgehoben werden.



Nutzen Sie den BITKOM Leitfaden „ASP Sicherheit“ Seiten 19 und 20, um die Angaben Ihres ASP-Partners zu bewerten.

Datenverlust und –missbrauch schadet nachhaltig dem Geschäft. Auch wenn ein Unternehmen nicht ursächlich daran beteiligt ist, verlieren seine Kunden oft das Vertrauen in die angewandten Geschäftsprozesse. Der Kunde sieht den Schaden, nicht die Ursache. Daher trägt der hohe Sicherheitsstandard Ihres ASP-Anbieters zur Zufriedenheit Ihrer Kunden bei.

Zusammenfassung

„Application Service Providing“ ist ein weit verbreitetes und erfolgreiches Geschäftsmodell in Deutschland, in Europa und weltweit.

Die Sicherheitsanforderung bei ASP verteilen sich auf Kunde und ASP-Anbieter:

- Anforderungen, die Sie selbst erfüllen müssen, ergeben sich grundsätzlich bereits durch Ihre Internetanbindung und sollten daher unabhängig von der ASP-Nutzung beachtet werden.
- Andere Anforderungen müssen von Ihrem ASP-Partner erfüllt werden. Bitte besprechen Sie die Einhaltung der Sicherheitserfordernisse mit Ihrem Dienstleister!

Mithilfe des BITKOM -„ASP Sicherheitsleitfadens“ können Sie prüfen, ob Ihre eigene IT-Umgebung und die Ihres ASP-Partners wirklich sicher sind.

Referenzen

BITKOM Leitfaden „Beispielvertrag für Application Service Providing“

BITKOM Leitfaden „Kompass der IT-Sicherheitsstandards“

BITKOM Leitfaden „ASP Sicherheitsleitfaden“

erhältlich bei:
BITKOM e.V.
Albrechtstr. 10
10117 Berlin-Mitte
Tel.: 030/27576-0
www.bitkom.org

Ihr Ansprechpartner:
Dr. Axel Garbers
Bereichsleiter Digitale Medien
und E-Dienste
Tel.: 030/27576-244
a.garbers@bitkom.org

ASP-Dienstleistungen und Sicherheit

HINWEIS:
Bitte beachten Sie auch die Notizen zu den Folien!

Anhang

BITKOM Leitfaden „ASP Sicherheitsleitfaden“ Übersicht (Ergänzung zu Folie 7)

Wie ist der Leitfaden aufgebaut?

Der Leitfaden strukturiert 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.

Gliederung der Maßnahmen:

- **Allgemeine Sicherheitsrichtlinien**
  - für Unternehmen und
  - für Mitarbeiter
- **Sicherung von Grundstück und Gelände**
- **Regelung des Zugriffsmanagements**
- **Identitätsmanagement (z.B. Passwörter)**
- **Virenprävention**
- **Schutz gegen Angriffe aus dem Internet**
- **Wartung der Systeme**
- **Sicherheit im LAN / WAN**
- **Authentifizierung am Server**
- **Verfügbarkeitskontrolle**
- **Backup-Management**
- **Ressourcen-Handling**