

# AK ASP Online Services Protokoll

Vertrauensfaktor Sicherheit –  
Vertrauen gewinnen durch gelebte Sicherheit  
13.06.2006

AK ASP Online Services Protokoll 13.06.06

Version 1.00

26.06.2006

eco  
Verband der deutschen  
Internetwirtschaft e.V.  
Lichtstr. 43h  
50825 Köln

Fon: +49 (0) 221-70 00 48-0  
Fax: +49 (0) 221-70 00 48-11  
info@eco.de  
www.eco.de

### **Begrüßung und Einführung ins Thema**

Arbeitskreisleiterin Stefanie Becker begrüßt die Teilnehmer und stellt das Thema der Sitzung vor: „Vertrauensfaktor Sicherheit – Vertrauen gewinnen durch gelebte Sicherheit“.

Obwohl sich das ASP-Geschäftsmodell momentan wieder im Aufwind befinde, seien die Sicherheitsbedenken der Anwender – unberechtigter Weise – noch immer sehr hoch. Ziel der Sitzung sei es daher, einerseits einen Überblick über die vorhandene Sicherheit von ASP-Lösungen zu bekommen – exemplarisch aufgezeigt an drei für ASP relevanten Sicherheitsthemen. Andererseits sollten Möglichkeiten diskutiert werden, wie diese bereits gelebte Sicherheit an den Kunden kommuniziert werden könne, um Vertrauen in ASP-Lösungen zu schaffen. Alle Teilnehmer seien eingeladen, ihre persönlichen Erfahrungen in die Diskussionen einzubringen.

### **Gelebte Sicherheit – Vertrauensbildung durch Audits und Zertifikate**

Im ersten Vortrag stellt Peter-Ralf Heinemann von der Nationalen Initiative für Internet-Sicherheit (NIFIS) e.V. die Möglichkeit vor, die in einem Unternehmen vorhandene Sicherheit mit Hilfe von Audits und den daraus resultierenden Zertifikaten zu belegen. Audits und Zertifikate könnten Unternehmen darin unterstützen, einen einmal erreichten Sicherheitsstandard zu halten und weiter zu optimieren. Derzeit gebe es auf dem Markt eine Vielzahl von Sicherheitszertifikaten, mit unterschiedlich hohen Komplexitätsgraden. Generell gelte, je höher der Komplexitätsgrad, desto höher der finanzielle und personelle Aufwand zur Durchführung des Audits. Viele, insbesondere kleinere, Unternehmen würden aus Kostengründen auf Audits verzichten. Dabei gebe es durchaus preiswerte Alternativen zu den Standardisierten Management-Zertifikaten auf Basis von ITIL oder IT-Grundschutz: Die so genannten Unabhängigen Systemzertifikate böten bedarfsorientierten Schutz bei geringem bis mittlerem Aufwand und hohem, sichtbarem Nutzen. Als Beispiel führt Herr Heinemann hier das eco Datacenter Star Audit und das NIFIS-Siegel an. Während das eco Datacenter Star Audit sich direkt an die Betreiber von Rechenzentren – und damit an die Anbieterseite – wende, sei das NIFIS-Siegel als allgemeiner Sicherheitscheck für Anbieter- und Nachfragerseite von Interesse. Diese Flexibilität des NIFIS-Siegels wird bei den Teilnehmern mit großem Interesse aufgenommen. Insbesondere wird diskutiert, das NIFIS-Siegel an ASP-Kunden weiter zu empfehlen, um die Sicherheit der ASP-Anwendungen von beiden Seiten aus zu erhöhen.

### **Technologische Sicherheit durch Kooperation mit Experten – Praxisbeispiel**

Im zweiten Vortrag stellt Herr Dr. Henry Hermann von Entrust Germany an einem Praxisbeispiel vor, dass auch der Einsatz der richtigen Technologie Vertrauen auf der

Anwenderseite schaffen kann. So suchte die Schufa AG, eine Kreditauskunftei mit mehr als 62 Mio. erfassten Personen, für ihr Webportal [www.meineschufa.de](http://www.meineschufa.de) ein Authentisierungsverfahren, das zum einen die hohen Sicherheitsanforderungen des Unternehmens erfüllen könnte und welches zum anderen die Anwender als sicher und gut bedienbar akzeptieren würden. Die seit Anfang des Jahres 2006 zunächst in einem Pilotprojekt eingesetzte Lösung „IdentityGuard“ von Entrust erfülle beide Bedingungen. Ähnlich einer Token-Lösung bekomme der Anwender eine kreditkartengroße Karte, die mit einer Matrix bedruckt sei. Melde er sich im Webportal an, werde er nach der Eingabe seines Benutzernamens aufgefordert, bestimmte Koordinaten der Matrix in das Webformular einzugeben. Diese Authentisierungsmethode sei intuitiv benutzbar und auch nicht technik-affine Nutzer würden den hohen Sicherheitsgrad der Lösung erkennen. Das Unternehmen indes profitiere ebenfalls vom hohen Sicherheitsgrad, von deutlich geringeren Kosten gegenüber einer Token-Lösung und vom Vertrauen der Nutzer. In der folgenden Diskussion werden die Potentiale und Einschränkungen dieser Lösung erörtert sowie mögliche Einsatzszenarien besprochen.

### **Rechtliche Sicherheit als Vertrauensfaktor**

In der dritten Präsentation der Sitzung, vorgetragen von RA Jens Eckhardt aus der Kanzlei Piepenbrock & Schuster, geht es um verschiedene Aspekte rechtlicher Sicherheit von ASP-Lösungen. Zunächst grenzt Herr Eckhardt den Begriff der rechtlichen Absicherung ggü. dem Begriff der Rechtssicherheit ab. Die rechtliche Absicherung sei die eigentliche vertragliche Regelung, die zum einen aus der Leistungsbeschreibung und zum anderen aus rechtlichen Regelungen zur Absicherung bestehe. Herr Eckhardt weist auf die besondere Wichtigkeit einer detaillierten Leistungsbeschreibung hin, denn nur was eindeutig geregelt und festgehalten sei, sei im Streitfall auch durchsetzbar. Die Regelungen zur rechtlichen Absicherung enthielten vertragliche Mittel (Sanktionen) zur Einhaltung der vereinbarten Leistungen. Diese Sanktionen könnten jedoch nur dann wirksam greifen, wenn konkrete Leistungsbeschreibungen vorlägen. Zudem dürften die Sanktionen dem Anbieter nicht günstiger sein als die Lieferung der vereinbarten Leistung. Als konkretes Beispiel einer Leistungsbeschreibung zieht Herr Eckhardt die Vereinbarung einer Verfügbarkeit heran. Im Anschluss werden weiterhin Haftungsfragen bei ASP-Verträgen, die Bedeutung einer Präambel bei Abschluss eines Vertrags sowie die Durchsetzbarkeit von Rechtsansprüchen im internationalen Recht bzw. die Funktion von Schiedsstellen besprochen. Als Fazit wurde festgehalten, dass eine transparente Vertragsgestaltung durchaus das Vertrauen des Kunden steigern kann, dass klare Leistungsbeschreibungen letzten Endes jedoch für beide Vertragsparteien von Interesse sind.