Zertifikat für SaaS-Lösungen

Providervergleich durch definierte Kriterien erleichtern

Frank Zscheile, freier Fachjournalist

Cloud und SaaS sind allgegenwärtig. Weil aber jeder Hersteller das Thema mehr oder weniger auf eigene Art und Weise definiert, bedarf es Standardisierungen. Der seit Mitte 2010 bestehende SaaS-EcoSystem e.V. hat vor kurzem mit der Initiative „Trust in Cloud" ein Instrument geschaffen, um eine solche Vergleichbarkeit herbeizuführen.

Der Zweck von Cloud-Standards ist es, eine bessere Vergleichbarkeit und höhere Zuverlässigkeit bei der dauerhaften Nutzung von Services zu erreichen. Anwender erhalten auf diese Weise Orientierung bei der Auswahl der für sie geeigneten Lösung. Verbindliche Cloud-Standards sind derzeit erst in der Entwicklung, im Bereich Security und Interoperabilität unter anderem von der Cloud Security Agency. Diese Standardisierung geht jedoch vom US-amerikanischen Markt aus und ist kaum auf hiesige Verhältnisse anwendbar.

Als deutsche Cloud-Initiative beschäftigt sich der SaaS-EcoSystem e.V. daher seit längerem mit der Schaffung von Standards, um Kundenunternehmen den Zugang zu SaaS-/Cloud-Services zu vereinfachen und eine Vergleichbarkeit zwischen Anbietern zu ermöglichen. Das Instrument hierfür heißt „Trust in Cloud" – ein Qualitäts-Zertifikat für SaaS und Cloud-Lösungen, an dem sich Anbieter entsprechender Lösungen freiwillig beteiligen können. Innerhalb eines Fragebogens können sie dort unter anderem angeben, welche Standards sie gegebenenfalls bereits unterstützen. So will der Verein die bislang noch im Aufbau befindliche Standardisierung im Cloud-Sektor fördern und Anwendern eine Brücke bauen.

Forum für Kunden und Anbieter

Der SaaS-EcoSystem e.V. wurde 2010 auf Initiative der IBM Deutschland als übergreifendes Netzwerk von Kompetenzträgern aus dem Bereich SaaS & Cloud in Frankfurt/Main gegründet. Er sollte Kunden und Anbietern ein Forum für innovative Technologien und Lösungen rund um SaaS & Cloud bieten. Der Verein unterstützt praxisorientiert die Nutzung von SaaS und Cloud Computing im deutschsprachigen Markt. Zu den Mitgliedern gehören Unternehmen wie IBM Deutschland, Computer Associates und Fujitsu Electronics. Wie Bernhard Braun, Programm Manager „Software-as-a-Service, Cloud Services" bei IBM Developer Relations erklärt, soll durch das SaaS-EcoSystem ein Experten-Netzwerk entstehen, das Softwareanbieter und Nutzer-Unternehmen gleichermaßen unterstützt.

Beim „Trust in Cloud"-Zertifikat können Anbieter ihre Leistungen anhand des Fragenkatalogs bewerten lassen. Im Gegensatz zu anderen Gütesiegeln wird die funktionale Qualität der Anwendungen nicht geprüft. Dies sei nicht zielführend, heißt es von Seiten des Vereins, da es hier an objektiven Kriterien und nachvollziehbaren und fairen Bewertungsrastern mangele. Das Zertifikat stelle vielmehr Ausstattungsmerkmale wie die Sicherheitsfunktionen und die Benutzbarkeit der Services für den Anwender in den Vordergrund.

Checkliste mit sieben Kriterien

Der Fragebogen listet sieben Bereiche: Referenzen, Datensicherheit, Entscheidungssicherheit, Qualität der Bereitstellung, Vertragsbedingungen, Service-Orientierung und Cloud-Architektur. Fünf Fragen werden innerhalb jedes Bereichs beantwortet. Pro positiver Antwort wird eine „Cloud" verliehen, für die Erlangung des Zertifikates sind drei Clouds pro Kategorie notwendig. Als neutrale Instanz prüft der Verein die Angaben der Hersteller nach verschiedenen Kriterien und stellt sie potenziellen Anwendern in

Form einer Checkliste kostenlos zur Verfügung. SaaS/Cloud-Anbietern bietet „Trust in Cloud“ gleichzeitig die Möglichkeit, sich über das neue Zertifikat am Markt zu positionieren.
Der Sicherheitsaspekt spielt in Sachen Cloud naturgemäß eine besondere Rolle. Das Zertifikat fragt in diesem Zusammenhang folgende Fakten ab:

- Ist die Verschlüsselung des Datenaustausches durch standardisierte bzw. allgemein anerkannte Sicherheitsverfahren (wie zum Beispiel SSL-Verschlüsselung, PKI-Verfahren etc.) gewährleistet?
- Lässt sich der Zugriff auf Daten und Funktionen für bestimmte Bereiche über eine Benutzer-Rechteverwaltung steuern und kontrollieren?
- Kann der Kunde jederzeit eine Kopie der Daten erstellen und diese in einem frei wählbaren Format herunter laden?
- Gibt es einen Prozess, der die kostenlose Übergabe der Daten an den Kunden und deren anschließende Löschung nach Vertragsbeendigung sicherstellt?
- Ist ein Datenschutzbeauftragter bestellt, der die Einhaltung der Datenschutzbestimmungen nach dem Bundesdatenschutzgesetzes überwacht?

Ein weiteres Kriterium betrifft die Qualität der Bereitstellung. Der Hersteller muss dazu darlegen, wie er die Performance der Anwendung in Bezug auf optimale Rechenleistung und Bandbreite auch bei hoher Transaktionslast sicherstellt. Gefragt wird ferner, ob der Betrieb der Anwendung und die Datenhaltung innerhalb der rechtlichen Bestimmungen stattfinden und ob die physische Infrastruktur durch Zugriffskontrollen gesichert ist. Weitere Fragen in diesem Bereich sind: Ist die Zusicherung der Hochverfügbarkeit für die Anwendung Bestandteil des Vertrages? Ist die Qualität der Zusicherung durch einen Prozentsatz transparent und mit anderen Lösungen vergleichbar? Wird eine permanente Datensicherung durch definierte Backup- und Recovery-Prozesse garantiert?

Sicherheit durch Unternehmenserfolg

Beim Kriterium „Entscheidungssicherheit“ geht es um die Marktdurchdringung des Anbieters und seines Produktes. Ist das anbietende Unternehmen älter als drei Jahre? Hat das anbietende Unternehmen im letzten Geschäftsjahr einen Gewinn erwirtschaftet? Wurden im letzten Geschäftsjahr mehr neue Kunden für SaaS / Cloud gewonnen als im Vorjahr? Wurde die Lösung bereits von einer anderen Organisation erfolgreich zertifiziert und wird damit geworben? Wurden in den letzten zwei Jahren regelmäßig alle Updates eingespielt?
Außerdem werden Kündigungsfristen, Haftungsregelungen und Einzelheiten des Kunden-Services dargestellt und schlussendlich vermittelt das Zertifikat auch technische Angaben zur Cloud-Architektur des Anbieters. So wird erläutert, ob die Lösung auf Internet-Standards basiert und ob sie eine browserbasierte Oberfläche oder eine App für mobile Endgeräte bietet. Geklärt wird, ob die Administration der Anwendung durch das Nutzer-Unternehmen erfolgen kann und ob gewährleistet ist, dass alle Kunden zu jeder Zeit mit dem gleichen Software-Release arbeiten. Auch die automatisierte Bereitstellung der Software ist ein Thema in diesem Bereich, ebenso ob die Lösungsarchitektur eine beliebige Skalierung, also die unlimitierte Nutzung der Anwendung, erlaubt? ■

Impressum

Informationsdienst IT-Grundschutz

6. Jahrgang – ISSN 1862-4375

Herausgeber
Nina Malchus

Redaktion
Elmar Török, Fachjournalist
(verantw. für den redaktionellen Teil)
Tel.: +49 89 381578030
E-Mail: redaktion@grundschutz.info

Verlag
SecuMedia Verlags-GmbH
Lise-Meitner-Str. 4, 55435 Gau-Algesheim
www.secumedia.de

Beteiligungsverhältnisse (Angabe gem. §9, Abs.4 Landesmediengesetz RLP) Gesellschafter zu je 1/6 sind Gerlinde Hohl, Klaus-Peter Hohl, Peter Hohl (GF), Veronika Laufersweiler (GF), Nina Malchus (GF), Stefanie Petersen.
Registereintragung: Handelsregister Mainz B 22282
Umsatzsteuer-Identifikationsnummer: DE 148266233

Abo-Service
Max Weisel
Tel.: +49 6725 9304-27
Fax: +49 6725 5994
E-Mail: aboservice@secumedia.de
www.grundschutz.info

Anzeigenleitung
Birgit Eckert
(verantw. für den Anzeigenteil)
Tel.: +49 6725 9304-20
E-Mail: anzeigenleitung@secumedia.de
Mediadaten unter: www.grundschutz.info

Bezugspreise/Bestellungen/Kündigung
Erscheinungsweise 8 Mal jährlich
Jahresabopreis für die Printausgabe:
98,00 € inkl. MwSt. u. Vers.k. (Inland) /
116,10 € inkl. MwSt. u. Vers.k. (Ausland)/
187,00 SFR inkl. MwSt. u. Vers.k. (Schweiz).
Einzelheft: 13,50 € inkl. MwSt.u. Vers.k. (Inland) /
16,00 € inkl. MwSt. u. Vers.k. (Ausland)/
27,50 SFR inkl. MwSt. u. Vers.k. (Schweiz).
Als e-paper Abo (PDF) 65,- € inkl. MwSt.

Eine Kündigung ist jederzeit zur nächsten noch nicht gelieferten Ausgabe möglich. Überzahlte Beträge werden rückerstattet.

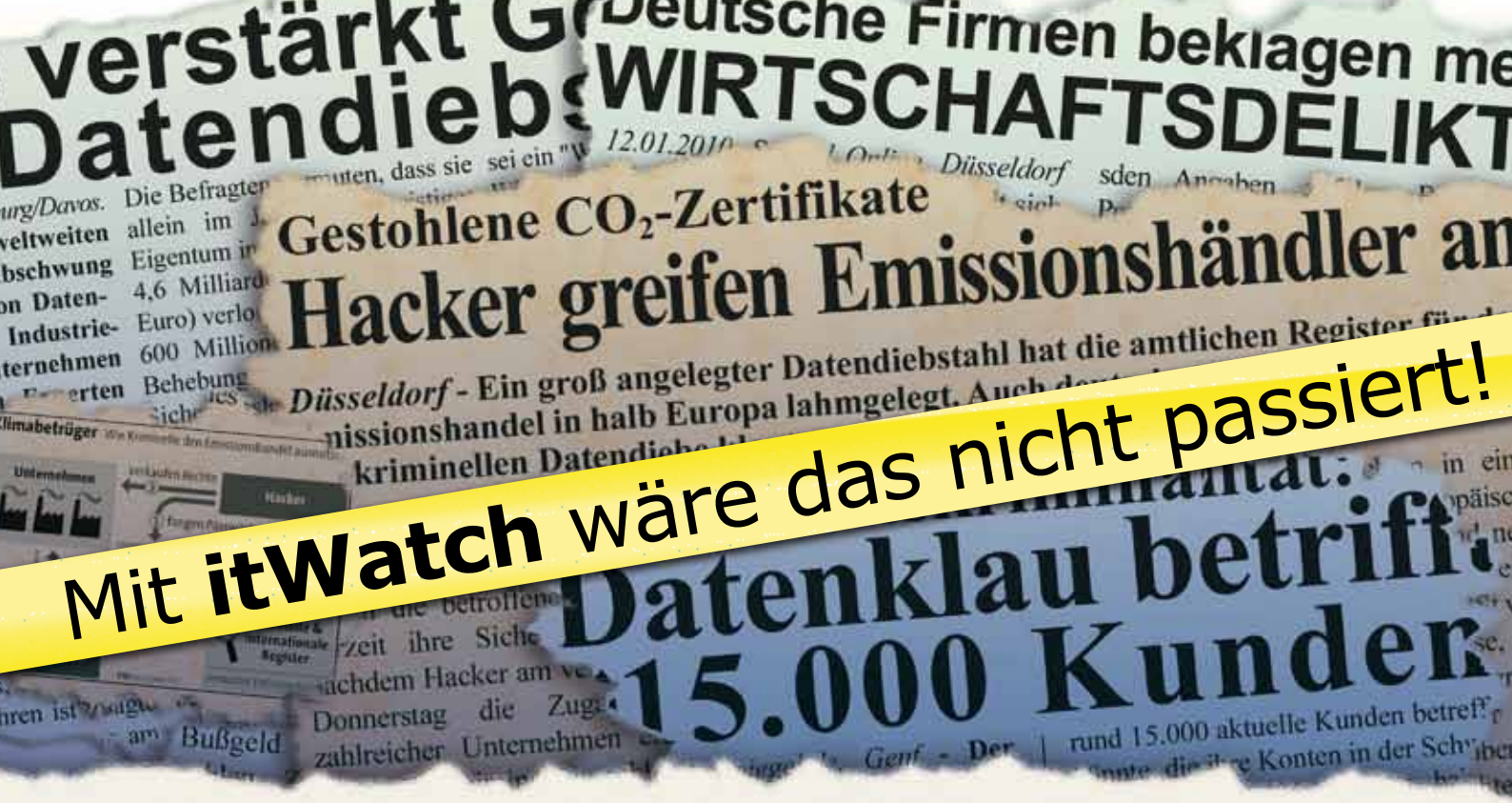
Preis im Koppelabonnement mit den Zeitschriften <kes> oder WIK:
Jahresabopreis: 76,00 € inkl. (Inland) / 84,53 € (Ausland) inkl. MwSt. und Versandkosten 130,00 SFr. (Schweiz)

Vertriebskennzeichen: ZKZ 78871

Satz/Druckvorstufe
BLACKART Werbestudio Schnaas und Schweitzer, Stromberger Str. 47, 55413 Weiler

Druck
Silber Druck oHG,
Am Waldstrauch 1, 34266 Niestetal

Titelbild: iStockphoto / billoxford



DLP Innovationen zu Ihrem Schutz

Endpoint Security

Portable Anwendungen auf USB-Stick, Synchronisation sensibler Daten via Bluetooth mit Smartphones, eingebaute UMTS oder WLAN Adapter, digitale Kameras - ein Gerätezoo, den es zu zähmen gilt. Den Administrationsaufwand senken, die Nutzungsszenarien monitoren, Geräte und Anwendungen inventarisieren und gleichzeitig die Sicherheit erhöhen.

Compliance

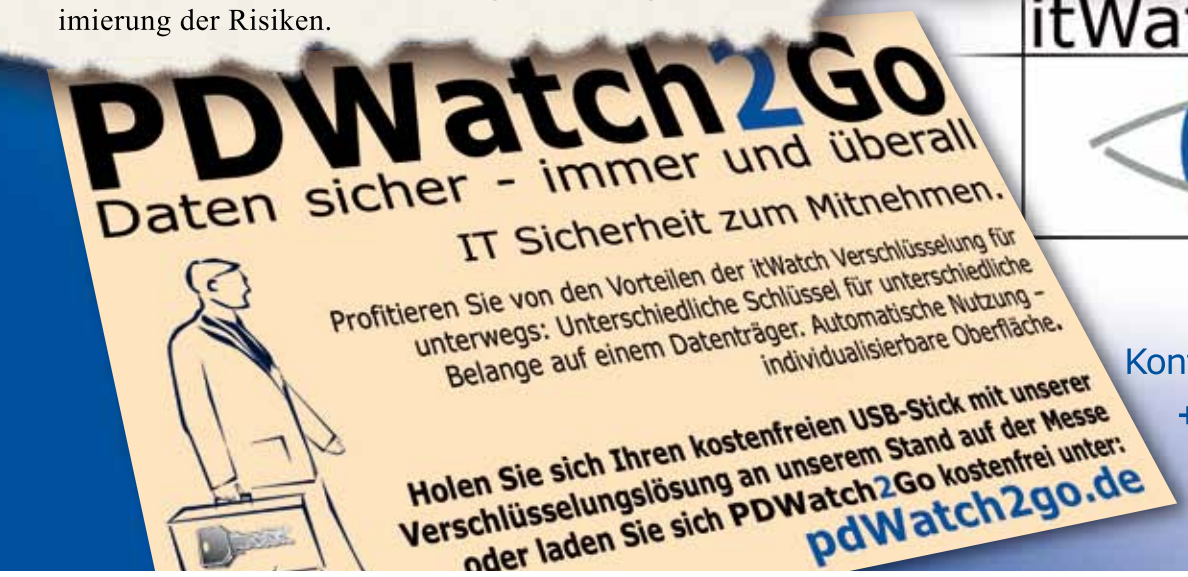
Memory Sticks, WLANs und sonstiger unerwünschter "Informations-Abfluss“ auf PCs und Notebooks sind nur einige der Risiken am Endpoint. Wer compliant zu SOX, Euro Sox, KonTraG, BDSG sein will, muss diese Risiken aktiv beherrschen. Gute Lösungen unterstützen technisch vollständig und dauerhaft beim Aufspüren unerwünschter Datenlecks und der Identifizierung, Bewertung und Minimierung der Risiken.

Security Awareness

Sicherheit und Compliance gegen die Anwender durchzusetzen ist teuer oder unmöglich - gemeinsam mit den Anwendern die Sicherheitskultur des Unternehmens durchsetzen, erfordert eine flexible Lösung mit VIP- und Selbstfreigabe-Funktionen.

Data Loss Prevention

Angriffe durch eingeschleuste Malware (LNK, PDF, IE, ZIP, Stuxnet …), mangelndes Risikobewusstsein der Anwender und vorsätzlicher Datendiebstahl sind Hauptursachen für den Verlust vertraulicher Informationen. itWatch schützt gegen jeden dieser Angriffe.



itWatch GmbH

Kontaktieren Sie uns:

+49 89 620 30 100
Info@itWatch.de
www.itWatch.de

2011: it-sa, PITS, Security Zone, Visit, it&business …
in Nürnberg, Berlin, Zürich, München, Stuttgart … www.itWatch.de/events