Multifaktorauthentifizierung als Sicherheitslösung aus der Cloud

Ergebnisse einer Delphi-Studie mit Experten des BITKOM-Netzwerks

BITKOM

UR

Impressum

Herausgeber: BITKOM
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner: Lutz Neugebauer
Tel.: 030.27576-242
l.neugebauer@bitkom.org

Autor: Christian Senk
Universität Regensburg
christian.senk@uni-r.de

Gestaltung/Layout: Design Bureau kokliko / Astrid Scheibe (BITKOM)

Titelbild: Daniela Stanek / Astrid Scheibe (BITKOM)

Multifaktorauthentifizierung als Sicherheitslösung aus der Cloud

Ergebnisse einer Delphi-Studie mit Experten des BITKOM-Netzwerks

BITKOM

Inhaltsverzeichnis

Zusammenfassung

Cloud Computing bietet sowohl Organisationen als auch Privatanwendern neue Optionen für den Bezug einer starken Benutzerauthentifizierung als fertige Lösung von einem spezialisierten Anbieter. Mittel- bis langfristig werden entsprechende Cloud-basierte Dienste, welche eine traditionelle passwortbasierte Authentifizierung durch Token-basierte oder biometrische Verfahren wahlweise ergänzen oder ersetzen, signifikant an Bedeutung gewinnen. Hierbei werden insbesondere Verfahren dominieren, welche sich auf den Besitz eines Hardware- oder Software-Tokens stützen. Organisationen werden Cloud-basierte Authentifizierungsdienste primär dort einsetzen, wo ein Anwendungsfall die Öffnung des Firmennetzes zum Internet erfordert. Dies umfasst die Authentifizierung von externen Partnern oder Firmenkunden (z.B. in Föderationen), die Authentifizierung von Privatkunden im öffentlichen Sektor und den Schutz betrieblicher (extern betriebener) Cloud-Anwendungen. Außerdem erweist sich Cloud Computing als attraktives Modell, um zentralisierte Identitäts- und Zugriffsmanagementsysteme im Unternehmen durch die Einbindung zusätzlicher Authentifizierungsverfahren funktionell zu erweitern. Für Privatnutzer spielen solche Dienste im Rahmen des dedizierten Schutzes einzelner kritischer Anwendungen (z.B. e-Banking, e-Governance) eine bedeutende Rolle. Primäre Erfolgsfaktoren Cloud-basierter Systeme für Multifaktorauthentifizierung sind deren einfache Bedienbarkeit sowie die Akzeptanz verwendeter Authentifizierungsverfahren, die einfache technische Integrierbarkeit, die Möglichkeit einer universellen geräteunabhängigen Nutzung sowie hohe Datensicherheit. Außerdem ist eine hohe Reputation bzw. Marktsicherheit des Dienstanbieters von essentieller Bedeutung für den Erfolg solcher Dienste.

Motivation

Zunehmender Praxisbedarf einer »starken« Benutzerauthentifizierung

Die sichere und zuverlässige Erkennung eines Benutzers ist essenziell für die korrekte Zuweisung von Benutzungsrechten und somit für eine effektive Kontrolle von Zugriffen auf Applikationen oder Web-basierte Dienste. Da sie einfach zu implementieren sind und isoliert betrachtet eine hohe Praktikabilität aufweisen, dominieren in der Praxis derzeit Authentifizierungsverfahren, die auf einem geheimen Wissensmerkmal (Passwort, PIN etc.) basieren. Das erreichbare Sicherheitsniveau einer solchen Benutzerauthentifizierung ist jedoch sehr begrenzt. Gründe sind die mangelnde menschliche Fähigkeit mit komplexen und somit hinreichend sicheren Kennwörtern umzugehen sowie deren beliebige Übertragbarkeit aufgrund fehlender Personenbindung. So werden solche wissensbasierten Methoden mittel- bis langfristig signifikant an Bedeutung verlieren und in Anwendungsfeldern mit erhöhtem Schutzbedarf zunehmend durch besitzbasierte (z. B. Chipkarten) oder auch durch biometrische Verfahren (z. B. Gesichtserkennung) zu einer »starken« Zwei- bzw. Multifaktorauthentifizierung ergänzt oder durch diese gar völlig ersetzt werden (siehe Abbildung 1).

Bisher mangelnde Verbreitung von Multifaktorauthentifizierungssystemen

Obwohl der Bedarf für eine Multifaktorauthentifizierung im Umfeld vieler Anwendungsfälle besteht, sind entsprechende Systeme noch wenig verbreitet. Ein möglicher Grund sind die verhältnismäßig hohen Kosten, die mit der Bereitstellung der notwendigen Infrastruktur, z. B. für biometrische Sensoren oder Chipkartenlesegeräte, verbunden sind. Auch mögliche Einbußen hinsichtlich der Benutzerfreundlichkeit oder aber Sicherheitsbedenken bremsen die Verbreitung »starker« Authentifizierungssysteme.

Cloud Computing als mögliche Lösung?

Cloud Computing ist ein Outsourcing-Modell, welches sowohl Unternehmen als auch Privatanwendern äußerst flexible Möglichkeiten für den Bezug bestimmter IT-Dienstleistungen von spezialisierten Anbietern verspricht. Dass sich dieses Modell auch auf IT-Sicherheitsanwendungen übertragen lässt und insbesondere aus Kosten- und Qualitätsgesichtspunkten ein hohes Marktpotenzial aufweisen, konnte bereits vergangenes Jahr (2011) durch eine BITKOM-Studie belegt werden. Im Rahmen der hierbei durchgeführten Unternehmensbefragung haben wir Daten erhoben, welche auch die Relevanz Cloud-basierter Dienste für Multifaktorauthentifizierung belegen. So planen bereits 12,8% der befragten Organisationen den Einsatz derartiger Dienste für die kommenden Jahre.

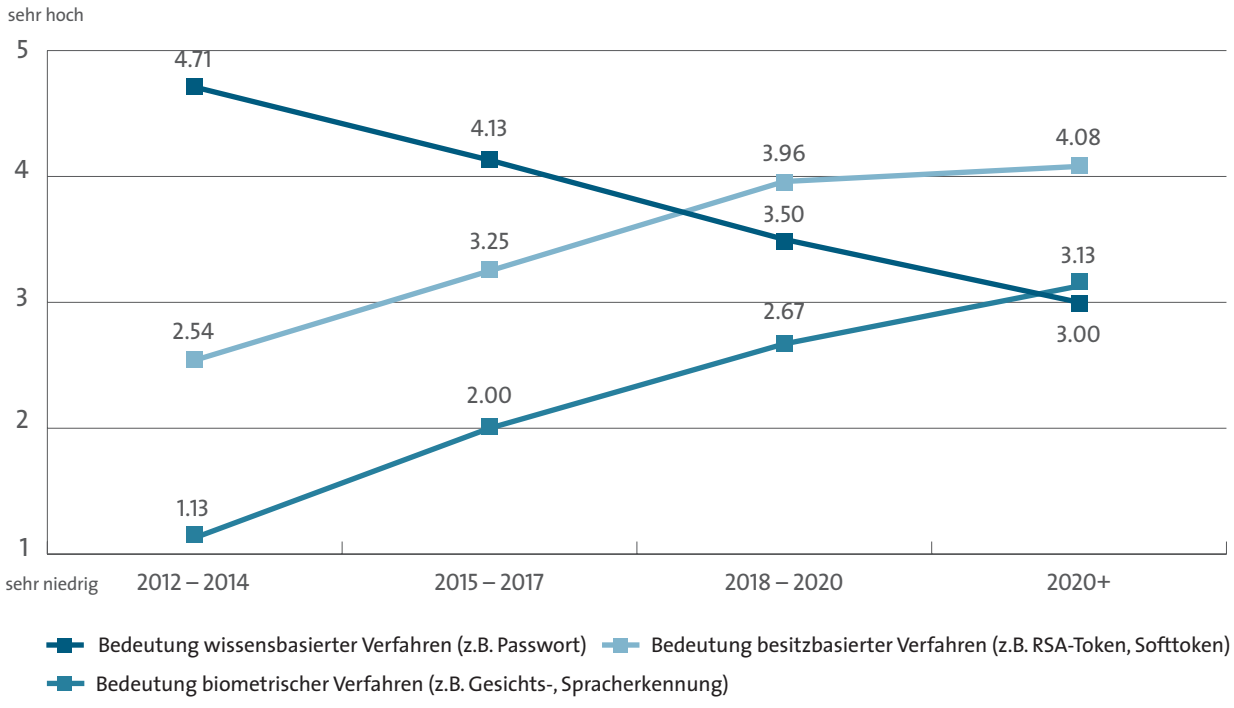

Abbildung 1. Entwicklung der Bedeutung möglicher Authentifizierungsansätze (n=24)

Entwicklung und relevante Authentifizierungsverfahren

Innerhalb der nächsten drei Jahre werden Cloud-basierte Authentifizierungsdienste lediglich eine untergeordnete Rolle spielen. Mittel- bis langfristig soll sich das jedoch signifikant ändern. Mit der abnehmenden Bedeutung der traditionellen wissensbasierten Benutzererkennung werden Systeme, welche auf alternativen Verfahren basieren immer wichtiger. Solche Systeme werden zu einem großen Teil als Sicherheitslösung aus der Cloud bezogen werden.

Den Kernbestandteil Cloud-basierter Dienste für eine starke Benutzerauthentifizierung bilden Methoden, welche auf dem Besitz eines Hardware-Tokens (z.B. Chipkarte, RSA-Token) oder Software-Tokens (z.B. Smartphone-App zur Generierung von Einmalpasswörtern) basieren. Passwörter und biometrische Verfahren wie Fingerabdruck-, Tippverhaltens- oder Gesichtserkennung ergänzen hierbei besitzbasierte Verfahren zu einer Multifaktorauthentifizierung, sowohl im Privatnutzer- als auch im Unternehmensumfeld.

Anwendungsfelder

Unternehmen werden Cloud-basierte Authentifizierungsdienste primär dann einsetzen, wenn ein Anwendungsfall die Öffnung des Firmennetzes zum Internet erfordert. So steht bei Bei Organisationen die Authentifizierung von Partnern und Geschäftskunden (z.B. für Single Sign-on in Föderationen) an erster Stelle, z.B. um überbetriebliche Sicherheitsinfrastrukturen zu vereinfachen oder zusätzliche Kontrollmöglichkeiten über den Cloud Service Provider als mögliche vertrauenswürdige dritte Instanz zu schaffen. An zweiter Stelle folgt Endkundenauthentifizierung im öffentlichen Bereich, d.h. Organisationen/ Behörden beziehen Cloud-basierte Authentifizierungsdienste vornehmlich, um Bürgern eine stärkere Authentifizierung zum Schutz ihrer Anwendungen und Prozesse zu ermöglichen (optional) bzw. durchzusetzen (verpflichtend). Weiterhin von Bedeutung ist der Schutz von organisationseigenen aber extern im Rahmen des Software-as-a-Service (SaaS) oder Application Service Providing (ASP) Modells betriebenen Softwareanwendungen. Diese Art der Anwendung liegt sehr nahe, da die zu schützenden Applikationen bereits außerhalb der eigenen Sicherheitsdomäne liegen und darüber hinaus einen hohen Grad an Standardisierung diverser Systemschnittstellen erwarten lassen, was wiederum eine einfache Integrierbarkeit sowie ein Anwendungsübergreifendes Single-Sign-on (außerhalb des eigenen Organisationsnetzwerks) ermöglicht. Das viertwichtigste Anwendungsfeld ist die funktionale Erweiterung betrieblicher Identitäts- und Zugriffsmanagementsysteme, welche zentralisiert ein organisationsweites Single-Sign-on für diverse Applikationen umsetzen. Hier kann das Cloud Computing-Modell dazu verwendet werden, bestehende Authentifizierungssysteme bedarfsweise und entsprechend kostenflexibel um stärkende, z.B. Token-basierte, Systeme zu ergänzen und somit den Authentifizierungsprozess technisch und wirtschaftlich flexibel zu stärken. Primäre Treiber für die Anwendung Cloud-basierter Systeme für starke Authentifizierung sind insbesondere geltende Compliance-Anforderungen. An zweiter Stelle folgen konkrete Anforderungen von Geschäftspartnern. Alle weiteren Faktoren werden nachrangig bewertet.

Für Dienstanbieter ergeben sich weitere Geschäftsmodelle durch eine direkte Adressierung privater Endkunden. Hier sehen die Experten den Schutz einzelner kritischer Anwendungen und Prozesse wie in den Bereichen e-Banking und e-Governance als lukratives Anwendungsfeld, da hier der Nutzer ein Eigeninteresse an hinreichend hoher Sicherheit verfolgt. Für weniger kritische private Anwendungen oder in Single Sign-On-Szenarien werden sich Cloud-basierte Authentifizierungsdienste hingegen nicht durchsetzen.

Erfolgsfaktoren

Zur Ermittlung der Erfolgsfaktoren wurden drei Ebenen unterschieden: Faktoren, die ein einzelnes Authentifizierungsverfahren betreffen, das zur Implementierung eines Multifaktorauthentifizierungssystems herangezogen werden kann; Faktoren, die das System selbst betreffen; und Faktoren, die sich auf den Anbieter auf organisatorischer Ebene beziehen.

Verfahrensebene

Der deutlich am kritischsten bewertete Faktor ist die Benutzerfreundlichkeit und -akzeptanz eines Verfahrens. Dieser wird von fast allen Experten als »äußerst kritisch« angesehen. Weiterhin sind auf Verfahrensebene die Transparenz und Datenschutzfreundlichkeit des Verfahrens von sehr hoher Bedeutung. Diese Anforderung spricht insbesondere gegen die Anwendung vieler biometrischer Verfahren, welche beispielsweise sensible Daten gemäß Bundesdatenschutzgesetz sammeln, speichern und verarbeiten.

Weitere wichtige Anforderungen sind die Unabhängigkeit eines Verfahrens von dedizierter clientseitiger Hard- oder Software von Bedeutung, sowie eine hohe erzielbare Stärke der Authentifizierung (durch die Anwendung des einzelnen Verfahrens). Die erwünschte Hard- bzw. Softwareunabhängigkeit schließt wiederum viele Verfahren aus, insbesondere solche, die eine dedizierte, im Anwendungskontext nicht breit standardisiert verfügbare Sensor- oder Lesegeräteinfrastruktur benötigen.

Systemebene

Auf Systemebene werden die Transparenz und Benutzbarkeit (des Gesamtsystems), Datensicherheit, die uneingeschränkte Nutzbarkeit auf diversen Endgeräten (z.B. Tablets oder Smartphones) sowie eine einfache Integrierbarkeit als am Kritischsten erachtet. Gerade die Anforderung der universellen Nutzbarkeit stellt wiederum Anforderungen an die zu implementierenden Verfahren. So muss beim Systemdesign z.B. berücksichtigt werden, dass Smartphones (noch) keine dedizierten und Leseschnittstellen für Smartcards oder RFID-Tags besitzen und vornehmlich auf Sprache und Bildgebung basierende biometrische Merkmale erfasst werden können. Trotzdem muss eine Nutzbarkeit des Systems, beispielsweise durch die Implementierung von Alternativverfahren gewährleistet sein.

Zweitrangig von Bedeutung sind: Schnittstellensicherheit, Hochverfügbarkeit, Kostenaspekte und eine hohe erzielbare Authentifizierungsstärke durch Anwendung implementierter Verfahren.

Anbieterebene

Primärer Erfolgsfaktor auf Anbieterebene ist die Reputation und Marktsichtbarkeit des Cloud Service Providers. Startup-Unternehmen mit möglichen innovativen Lösungsansätzen haben es somit, auch bei umfassender Zertifizierung, deutlich schwerer als bereits etablierte Player.

Weitere, sekundäre Erfolgsfaktoren sind das Angebot flexibler und kundenorientierter Lizenzmodelle um (a) mögliche Kostenvorteile zu generieren und (b) Einstiegs- und Wechselbarrieren möglichst niedrig zu setzen, sowie die externe Auditierbarkeit des Anbieters.

Abbildung 2 systematisiert die ermittelten Erfolgsfaktoren anhand der drei Betrachtungsebenen (Verfahren, System, Anbieter) und relevanter Akzeptanzdimensionen (Nutzen, Barrierefreiheit, Risiko). Primäre Erfolgsfaktoren werden durch Rechtecke mit durchgehenden Rahmenlinien dargestellt, sekundäre weisen gestrichelte Rahmenlinien auf. Zudem wurden die Faktoren inhaltlich gruppiert.

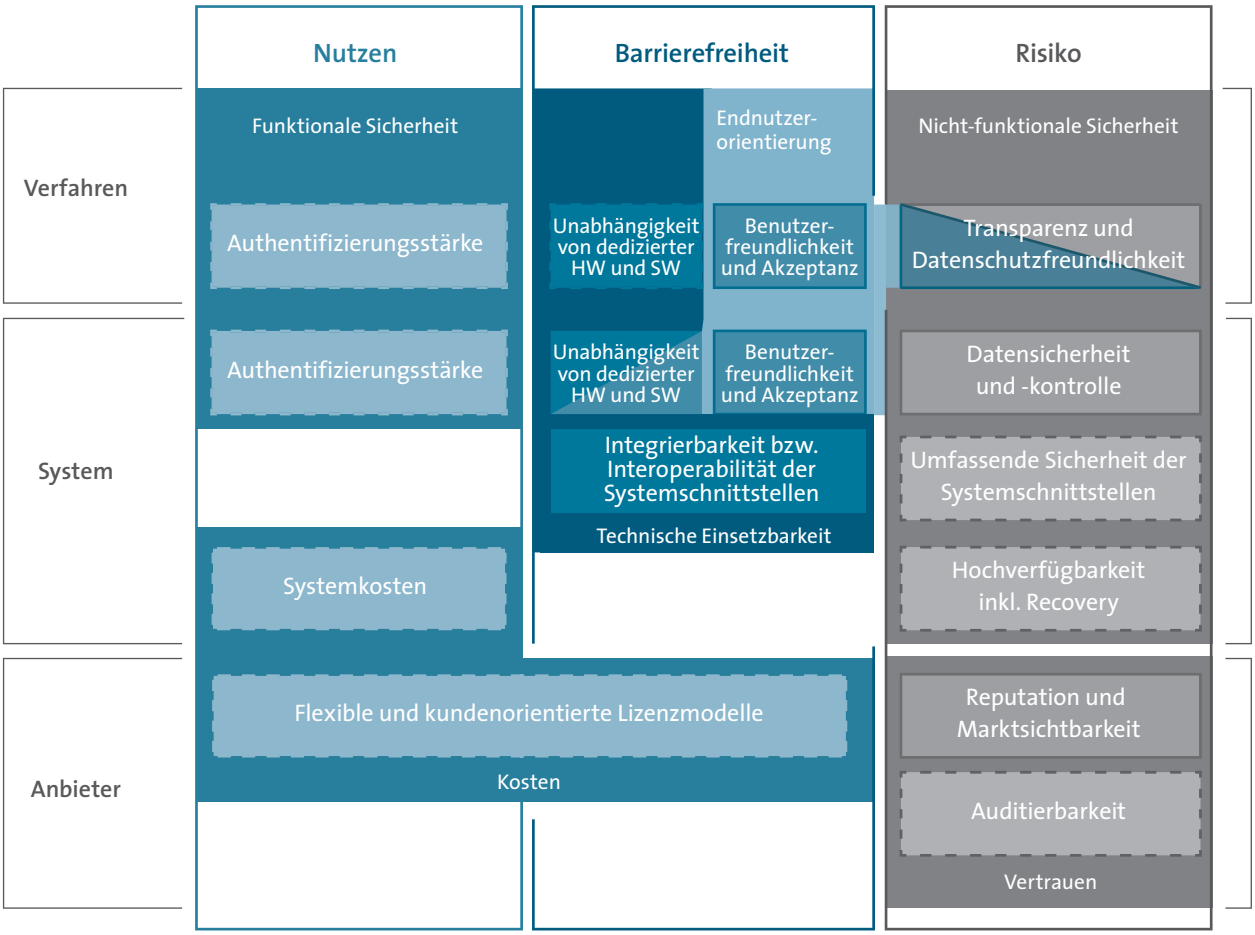

Abbildung 2. Einordnung ermittelter Erfolgsfaktoren

Anhang

Zur Methodik

Im Rahmen einer Expertenstudie sollten insbesondere die Relevanz, relevante Einsatzfelder sowie Erfolgsfaktoren von in der Cloud betriebenen Systemen für eine »starke« Benutzerauthentifizierung untersucht werden. Hierzu wurden 24 Experten aus unterschiedlichen Fachgebieten insgesamt dreimal gemäß der sog. Delphi-Methode befragt. Die Befragung fand zwischen Januar und April 2012 statt.

Danksagung

Besonderer Dank geht nicht nur an die zahlreichen Experten aus Industrie und Forschung, welche durch ihre Teilnahme diese Studie überhaupt erst ermöglicht haben, sondern auch an das Forschungsprojekt SkIDentity, das uns bei der Durchführung der Studie sowohl inhaltlich als auch organisatorisch unterstützt hat.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.700 Unternehmen, davon über 1.200 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu gehören fast alle Global Player sowie 800 leistungsstarke Mittelständler und zahlreiche gründergeführte, kreative Unternehmen. Mitglieder sind Anbieter von Software und IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien und der Netzwirtschaft. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org