

# Bedrohungen im Umgang mit Web 2.0

Sebastian Feld, Norbert Pohlmann, Sebastian Spooren

[feld | pohlmann | spooren]@internet-sicherheit.de

## Institut für Internet-Sicherheit

Fachhochschule Gelsenkirchen, Fachbereich Informatik

Neidenburger Straße 43, 45877 Gelsenkirchen

## Abstract

Web 2.0 scheint für die vernetzte Wissens- und Informationsgesellschaft neue und interessante Anwendungs- und Geschäftsmöglichkeiten zu bieten. Dazu müssen – wie bei jeder neuen Technologie – auch die Gefahren und Risiken, wie der Umgang mit vertrauenswürdigen Daten, analysiert und berücksichtigt werden. Um die mit dem Einsatz der Web 2.0 Technologie verbundenen Gefahren und Risiken auf ein mögliches Minimum zu reduzieren, müssen die Nutzer solcher Lösungen auf Basis von Sicherheitsplattformen, wie zum Beispiel Turaya, auf ein sehr viel höheres Level der Vertrauenswürdigkeit von IT-Systemen aufbauen, damit ein weiterer Fortschritt im Internet ermöglicht werden kann. Im Artikel werden dazu technische Sicherheitsmaßnahmen aufgezeigt und der Umgang mit Web 2.0 in punkto Sicherheit auf unterschiedlichen Ebenen ausführlich diskutiert.

---

**Inhaltsübersicht**

1. Einführung.....	3
2. Öffentliche Dienste im World Wide Web .....	4
3. Internetbasierte Groupwaredienste .....	9
4. Desktop-Simulationen .....	13
5. Basissicherheit für Anbieter von Webanwendungen.....	17
6. Tipps im Umgang mit Web 2.0 für den Benutzer.....	17
7. Ausblick.....	19

## 1. Einführung

Wir erleben zurzeit einen fundamentalen Wandel in eine Informations- und Wissensgesellschaft. Dabei müssen sich die Menschen bewusst werden, dass immer mehr Arbeitsabläufe mit Hilfe von Rechnersystemen, wie PCs, Notebooks und SmartPhones über das und mit Hilfe von Diensten im Internet abgewickelt werden. Damit nimmt auch die Notwendigkeit zu, IT-Sicherheitsmaßnahmen in angemessener Weise zu verwenden, damit im Internet eine Basis der Vertrauenswürdigkeit herrschen kann.

Wichtig ist die Erkenntnis, dass in den letzten Jahren die Sicherheitsprobleme im Internet von ihrer Bedeutung nicht kleiner, sondern sehr viel größer geworden sind.

Das gilt umso mehr, wenn der immer weiter steigende Wert elektronischer Informationen in Betracht gezogen wird. Dieser Wandel führt dazu, dass immer öfter finanziell wertvolle Daten auf Rechnersystemen gespeichert oder durch das Internet übertragen werden. Dazu zählen persönliche Daten, Entwicklungsunterlagen, Kundendaten, Logistikinformationen oder auch Strategiekonzepte, die z.B. Börsenwerte beeinflussen können. Solche Bits und Bytes können leicht mehrere Millionen Euro wert sein.

Eine weitere Herausforderung ist das häufig mangelnde Unrechtsbewusstsein in der elektronischen Welt. Wer in der realen Welt (Unternehmens-)Werte entwenden will, der muss über Zäune klettern, Türen und Fenster aufbrechen, vielleicht sogar Tresore sprengen. Jedem, der so etwas tut, ist bewusst, dass er eine Straftat begeht! In der elektronischen Welt sitzen die Hacker bzw. Cracker mit Kaffee und Keksen vor dem Bildschirm und machen das Gleiche, aber sie haben dabei häufig nicht das Gefühl, etwas unrechtes zu tun. Die Hemmschwelle ist niedriger, dadurch steigt die Wahrscheinlichkeit von Angriffen [Pohl02a].

Das Internet erstreckt sich ohne Rücksicht über alle geographischen, politischen und administrativen Grenzen und Kulturen. Damit stellt es eine neue und ungewohnte Herausforderung für die internationale Gesellschaft dar. Die Geschwindigkeit, in der neue Anforderungen auftauchen wird immer rasanter, was einen Anstieg des damit verbundenen Sicherheitsrisikos zur Folge hat.

Die größte Herausforderung besteht darin, für eine notwendige und passende Vertrauenswürdigkeit des Internets und seiner Dienste zu sorgen.

### **Welchen Schutzbedarf müssen wir berücksichtigen?**

***Gewährleistung der Vertraulichkeit:***

Damit keine unautorisierten Personen in der Lage sind, übertragene und gespeicherte Daten zu lesen.

***Gewährleistung der Authentikation:***

Damit wir bei einer elektronischen Kommunikation oder Transaktion wissen, wer unser Partner ist beziehungsweise wer auf unsere Betriebsmittel und Daten zugreift.

***Gewährleistung der Integrität:***

Damit wir überprüfen können, ob übertragene und gespeicherte Daten unverändert, dass heißt im Originalzustand sind.

***Gewährleistung der Verbindlichkeit:***

Damit wir die Gewissheit haben, dass die elektronischen Prozesse und die damit verbundenen Aktionen auch verbindlich sind.

***Gewährleistung der Verfügbarkeit:***

Damit wir die Gewissheit haben, dass die Daten und Dienste auch zur Verfügung stehen.

Aus dem Persönlichkeitsrecht:

***Informationelle Selbstbestimmung:***

Das Grundrecht zu haben, grundsätzlich selbst über die Preisgabe und Verwendung der eigenen persönlichen Daten zu bestimmen.

## **2. Öffentliche Dienste im World Wide Web**

Das Web 2.0 ist unter anderem dadurch definiert, dass es keinen erkennbaren Unterschied mehr zwischen Nutzer und Autor von Informationen gibt. Ein Anbieter stellt lediglich die Infrastruktur mit ihren Diensten zur Verfügung und die Nutzer bearbeiten die Inhalte. Zum Beispiel sammeln die Nutzer Informationen in Form von persönlichen, aber öffentlichen Linklisten, so genannten „Social Bookmarkings“. Eine andere Form von öffentlichen Diensten im Internet ist das „Social Networking“, bei welchem sich Nutzer auf verschiedene Arten kennen lernen und miteinander vernetzen. In Abbildung 1 wird exemplarisch gezeigt, dass verschiedene Benutzer je nach Interesse unterschiedliche Content-Dienste in Anspruch nehmen können, um Informationen auszutauschen oder Wissenswertes für die Allgemeinheit zu veröffentlichen.

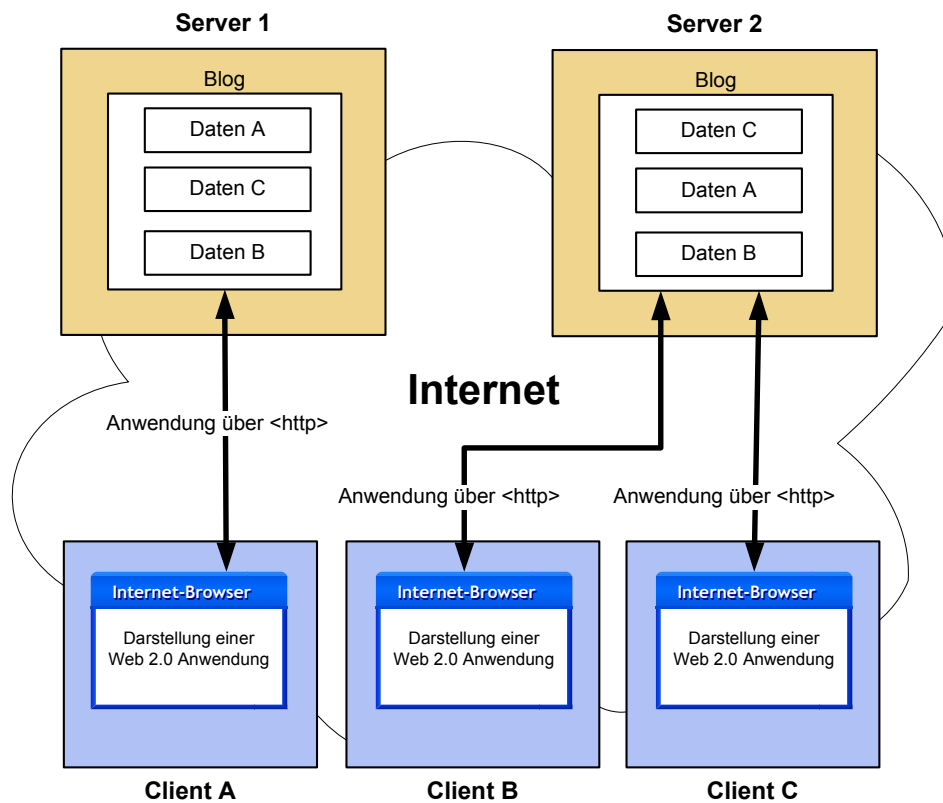


Abbildung 1: Content-Dienste auf Basis der Web 2.0 Technologie

Auf Basis des Web 2.0 werden immer mehr Informationen generiert und den Mitmenschen zur Verfügung gestellt. Dieser Prozess ist besonders bei Blogs, Wikis oder Tausch-Seiten von Bildern oder Videos zu beobachten. Ein Wiki ist eine Seitensammlung im Internet, die nicht nur von jedem gelesen, sondern auch von jedem verändert werden kann. Alle diese neuen Anwendungsmöglichkeiten sind nur möglich, da das Internet eine weite Akzeptanz gefunden hat. Die Hemmschwelle, neue Anwendungen im Internet auszuprobieren, ist gesunken, sodass viele Anwender den neuen Angeboten offen entgegen sehen. Daneben ist es durch die Breitband-Anbindungen nun möglich, Informationen nicht mehr nur in Textform, sondern auch als Audio- oder Videodatei zu veröffentlichen.

Diese positiven Entwicklungen haben natürlich auch eine Kehrseite. Die zahlreichen, freiwillig preisgegebenen Informationen sind für jedermann einsehbar. Nicht nur Freunde oder Bekannte, sondern zum Beispiel auch Personalchefs können diese Daten lesen. Aber auch nicht öffentlich freigegebene Informationen können Sorgen bereiten. Sind die Server des Anbieters hinreichend geschützt? Werden personenbezogene Informationen an Dritte weitergegeben? Ein weiterer Punkt sind die vom Nutzer generierten und veröffentlichten Inhalte. Wie ist die rechtliche Situation? Wem gehören die Kommentare in Blogs, die Blogeinträge, hochgeladene Videos oder zur Schau gestellte Bilder?

Im Folgenden werden alle diese Fragen szenariobasiert erörtert:

### 1.1. „Social Networking“ mit Blick auf Datenschutz und Datensicherheit

Unter „Social Network“-Anwendungen werden meist freie Dienste im Internet verstanden, bei denen ein Nutzer Informationen über sich selber einspielt. Dies sind zum Beispiel persönliche Angaben, wie Hobbies, Musikgeschmack oder favorisierte Webseiten, aber auch selbst-erstellte Fotografien, Videos oder andere Inhalte. Über diese Selbstbeschreibung der bei diesem Dienst angemeldeten Nutzern können leicht alte Freunde wieder gefunden werden, neue Freundschaften geknüpft oder Gruppen entstehen, welche die gleichen Interessen teilen. All dies geschieht freiwillig und auch recht großzügig. Denn je mehr jeder einzelne von sich preisgibt oder je aktiver jeder einzelne sich in der virtuellen Szene bewegt, desto stärker wird er wahrgenommen.

Dieser Aspekt des „Social Networkings“ wirft sofort die Frage auf, wie es mit der informationellen Selbstbestimmung steht. Werden persönliche Daten analysiert oder gar an Dritte weitergegeben? Nicht selten besteht das Geschäftsmodell einiger Dienstanbieter aus der Weitergabe von anonymisierten Daten, welche Profile oder Statistiken über die Nutzung von spezifischen Seiten enthalten. Die Handhabung des Datenschutzes wird von jeder Web 2.0 Anwendung explizit erklärt. So gibt es Anbieter, die darauf achten, dass die strengen Datenschutzgesetze an oberster Stelle stehen und personenbezogene Daten geschützt werden. Andererseits gibt es auch Dienstanbieter, die die Weitergabe dieser kritischen Informationen ausdrücklich erwähnen, etwa um gesetzliche Bestimmungen zu erfüllen, die Nutzungsbedingungen durchzusetzen oder um die Rechte des Anbieters zu schützen.

Neben den scheinbar anonymen Bewegungsprofilen besteht außerdem die Gefahr, dass aus einer Kombination der persönlichen Nutzerinformationen und den Verlinkungen innerhalb eines Netzwerkes regelrechte Soziogramme erstellt werden. Das möglichst genaue Abbilden der eigenen Person im Netzwerk hat allerdings auch seine Schattenseiten, wenn die persönlichen Informationen ausgenutzt werden. Ein Beispiel bietet der Personalchef, der sich einen Eindruck von einer Person einholt, bevor er diese zum Bewerbungsgespräch einlädt. Die Möglichkeit, indirekt und relativ anonym neue Kontakte zu knüpfen, ist ein weiterer Aspekt des „Social Networkings“, welcher missbraucht werden kann. Er kann zum Beispiel von Triebtätern genutzt werden, welche über diesen Weg Minderjährige ansprechen und somit versuchen, Kontakte aufzubauen. Vorfälle dieser Art werden von Behörden als Anstoß genutzt, um die Profildatenbanken der betroffenen Dienste mit Daten von Sexualstraftätern oder sonstigen Vorbestraften abzugleichen. Dieses eigentlich positive Vorgehen wirft aber erneut die Frage auf, ob der Datenschutz tatsächlich gegeben ist oder ob die Anwender zu gläsernen Menschen werden. Welche Erkenntnisse sind möglich, wenn man vorhandene Profile mit Datenbeständen wie zum Beispiel Handyabrechnungen oder Finanzbewegungen abgleicht? An dieser Idee, bekannt unter dem Namen „Semantic Web“ [DOS03], arbeitet un-

ter anderem die Internetgemeinde selbst. Gespeicherte Informationen sollen gleichermaßen vom Mensch, als auch von Maschine gelesen und verstanden werden. Wird die Forschung in diese Richtung Erfolg haben, so können die erwähnten Datensätze kombiniert und regelrechte Rasterfahndungen betrieben werden.

Das eben diskutierte Thema bezüglich der Ungewissheit des Gegenübers offenbart eine weitere Problematik, die im Einklang mit dem fehlenden Sicherheitsbewusstsein vieler Nutzer steht: Große Web 2.0-Anwendungen, genauso wie Internet-Auktionshäuser und viele weitere Anwendungen, sind attraktiv für das Ausspähen von Nutzerdaten, wie etwa durch Phishing-Attacken [HePo06]. Die erspähten Zugangsdaten werden beispielsweise benutzt, um das Profil des Betroffenen zu manipulieren. Dies hat zumeist einen großen „sozialen“ Schaden für die Person zur Folge. Des Weiteren ist die Wahrscheinlichkeit groß, dass der Geschädigte dieses Passwort für mehrere Dienste im Internet benutzt, was zu weiteren Schäden führen kann – zum so genannten „Identitätskollaps“ [LiPo05].

## 1.2. „User-generated Content“ und die rechtliche Situation

Im Web 2.0 gibt es im Prinzip keine konkrete Unterscheidung zwischen Nutzer und Autor von Informationen. Jeder ist angehalten mitzumachen, Texte zu veröffentlichen und zu kommentieren, Informationen zu sammeln oder zu tauschen. Diese vom Nutzer eingestellten Inhalte werden auch „user-generated content“ genannt und es stellt sich die Frage, wem die Inhalte gehören oder welche Lizenzen oder Rechte gelten. Hierfür gibt es einige Ansätze, wie zum Beispiel die „Creative Commons-Lizenzen“. Dies sind Lizenzen mit starken Abstufungsgraden, die von fast vollständigem Vorbehalt der Rechte bis hin zum völligen Verzicht auf Urheberrechte reicht, sprich Gemeinfreiheit. Hierzu werden drei Fragen mit ja oder nein beantwortet, nämlich ob die Nennung des Urhebers vorgeschrieben oder eine kommerzielle Nutzung der Inhalte erlaubt ist oder ob Veränderungen erlaubt sind. Mit diesen Lizenzen kann beispielsweise für das eigene Internet-Tagebuch (Blog) festgelegt werden, was genau mit den veröffentlichten Inhalten passieren darf. Eine nicht ohne weiteres zu beantwortende Frage ist die, wem die zahlreichen Kommentare in den Blogs gehören. Dieser Offenheit kann beispielsweise damit entgegnet werden, indem mit Hilfe der „Creative Commons-Lizenzen“ in den AGBs festgelegt wird, dass sämtlicher Inhalt des Blogs, also alle Blogbeiträge, sowie die Kommentare der Besucher, nicht kommerziell verwendet, verändert, aber mit Nennung des Urhebers zitiert oder anderweitig publiziert werden dürfen. Ist ein Kommentator mit dieser Regelung nicht einverstanden, so muss er für sich entscheiden, ob er seinen Kommentar abgibt, oder aber einen eigenen Blogbeitrag schreibt und auf den entsprechenden Blog verweist.

Ein anderer Bereich, in der die rechtliche Situation bezüglich der Inhalte von großer Bedeutung ist, sind Dokumente, die der Allgemeinheit über Wikis zugänglich gemacht werden. Das im Internet sehr bekannte Beispiel Wikipedia zeigt, dass eine Gruppe interessierter Menschen sogar eine ganze Enzyklopädie erstellen kann. Hier kommt eine GNU-Lizenz zum Tragen, nämlich die GNU-Lizenz für freie Dokumentation, GNU-FDL. Dies ist eine Lizenz für „freie Inhalte“, die besagt, dass der Autor, also der Urheber der Information, keine Vergütung erhält und die Verbreitung ausdrücklich erwünscht. Der Autor stellt den Inhalt jedem zur Verfügung, macht ihn also gemeinfrei, solange ein Dritter mit der Benutzung, Vervielfältigung, Verbreitung oder Veränderung des Inhalts dieselbe Lizenz einhält, spricht erneut Gemeinfreiheit bewahrt.

### **1.3. Content-Storing and -Sharing**

Das Anbieten von Online-Ressourcen zum Speichern von Bildern und Videos, sowie das Tauschen derselben, ist eine weitere große Ausprägung vieler Web 2.0-Anwendungen. Die Nutzer können ihre Dokumente auf die Server des Anbieters laden und haben somit den Vorteil, von überall aus auf die Daten zugreifen zu können. Außerdem kann dieser Service als ein Backup der lokalen Daten betrachtet werden. Nicht private Fotos oder Videos können der Allgemeinheit zugänglich gemacht werden, es wird auch hier über Inhalte diskutiert, verlinkt oder sich zu Gruppen zusammengeschlossen. Besonders Video-Plattformen erfahren derzeit großes Interesse. Mittels Videobotschaften bieten die Autoren ihre individuellen Videos, beispielsweise ihr Tagebuch, im Internet allen Interessierten zum Download an.

Interessant ist hierbei die Betrachtung der vom Anbieter beanspruchten Rechte und Lizenzen. Diese sind bei den Storing- und Sharing-Angeboten unterschiedlicher Natur. Es gibt Anbieter, die sich komplett vom übertragenen Inhalt distanzieren und keinerlei Haftung übernehmen. Andere Anbieter beanspruchen weitgehende Rechte und Lizenzen für Veränderung, Verkauf, Vervielfältigung oder Verbreitung der Inhalte. Beide Seiten haben allerdings gemein, dass sie voraussetzen, dass der Nutzer des Dienstes die Rechte für den eingestellten Inhalt besitzt, sowie dass der Inhalt nicht gegen geltende Rechte verstößt.

Nutzt nun jemand dieses Angebot als Online-Festplatte oder als Backup-Möglichkeit, hat derjenige keine Gewährleistung, dass die Daten unverändert, verfügbar und somit sicher sind. In den Nutzungsbedingungen und AGBs wird meist nur vage auf diese Punkte eingegangen. Schwammige Formulierungen wie: „Wir fahren öfter Backups, als Sie die Dateien ändern können“ geben dem Nutzer des Dienstes keine Sicherheit; auch wird die Integrität, sowie die Verfügbarkeit nur indirekt angesprochen. Harte Fakten wie Verschlüsselung, Übertragungssicherheit oder Verfügbarkeit werden weder konkret angesprochen noch garantiert.

Wie die Beispiele und Sichtweisen gezeigt haben, sind die Möglichkeiten der neuen Web 2.0 Dienste, sowie die Situation der Rechte im Internet für die meisten Nutzer undurchsichtig und schwer nachvollziehbar. Das bedeutet, dass sich ein Nutzer genau überlegen sollte, welche Informationen er ins Internet stellt. Des Weiteren muss die Tatsache berücksichtigt werden, dass das Internet nichts vergisst. Das bedeutet, dass alle Informationen sehr lange im Internet gespeichert werden und im Regelfall für alle Interessierten jederzeit verfügbar sind.

### 3. Internetbasierte Groupwaredienste

Durch die Mobilitätsanforderungen der Mitarbeiter/Organisationen von Unternehmen und die zunehmende Zusammenarbeit in globalen Verbänden, wird der Wunsch nach zentralen Diensten, die über das Internet einfach verfügbar sind, immer größer.

Besonders wünschenswerte Dienste sind gemeinsame Terminkalender, Kontaktdaten, Dokumente und Projektpläne.

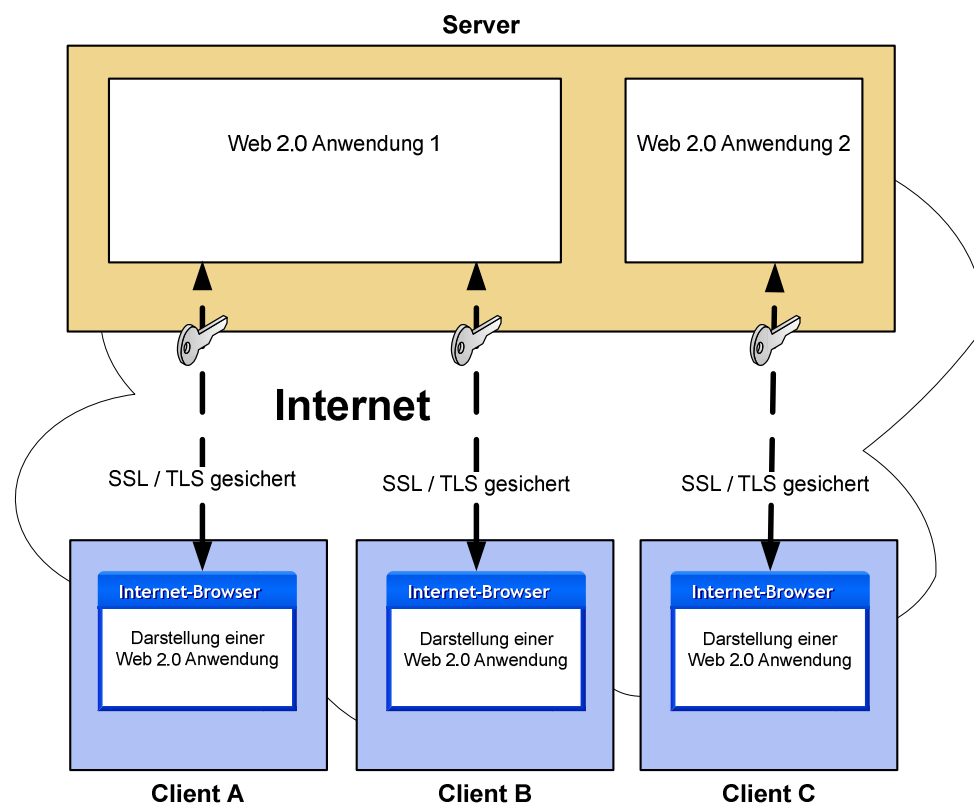


Abbildung 2: Groupwaredienste auf Basis der Web 2.0 Technologie

Da es sich in diesem Bereich um besonders sensible Daten handelt, muss sowohl der Zugriff auf solche Dienste als auch die Übertragung der Daten speziell gesichert werden.

Dabei spielen die Identifikation und Authentikation der berechtigten Nutzer sowie die Verschlüsselung der Kommunikation eine wichtige Rolle.

## **Identifikation und Authentikation von Nutzern**

Die **Identifikation** ist die Überprüfung eines vorgelegten, kennzeichnenden Merkmals, z.B. des Nutzernamens. In der realen Welt wird eine Person eindeutig durch die Angabe von Vorname, Nachname, Geburtsort und Geburtstag identifiziert. In Deutschland wird die Eindeutigkeit der Identifikation von den Standesämtern garantiert.

Eine Identifikation muss immer innerhalb eines Systems (Organisation, Nutzergemeinden, Dienstanbieter und so weiter) abgesprochen sein, damit sie eindeutig ist. Damit eine solche Absprache mit verschiedenen Nutzern zustande kommt, müssen klar definierte Regeln eingehalten werden. Dazu gibt es verschiedene Strategien für unterschiedliche Anwendungsszenarien.

**Authentikation** bezeichnet einen Prozess, in dem überprüft wird, ob »jemand« oder »etwas« echt oder berechtigt ist. Authentikation bedeutet die Verifizierung (Überprüfung) der Echtheit bzw. der Identität. Die Überprüfung des Personalausweises einer Person ist in der realen Welt eine solche Authentikation.

Was muss und kann z.B. in der IT-Welt identifiziert und authentisiert werden?

Kommunikationspartner: z.B. Nutzer, Anwendungen, Dienste, Instanzen, und so weiter oder Kommunikationsmedien: z.B. Client- und Serversysteme, usw. oder Nachrichten: z.B. Mails, Dateien, Java-Applets und weitere.

In der IT-Welt gibt es vier generelle Authentikationsmethoden.

**Passwort-Verfahren:** Das Passwort-Verfahren ist das einfachste Authentikationsverfahren. Ungünstig ist, wenn das Passwort im Klartext über das Internet übertragen wird, dann kann es mitgelesen und missbräuchlich verwendet werden. Aus diesem Grund ist es wichtig, dass das Passwort nur über eine verschlüsselte Kommunikation eingegeben wird. Außerdem müssen gewisse Passwortregeln eingehalten werden, damit möglichst kein Angriff möglich ist. Passwortregeln sind z.B.: Nirgends notieren! Niemandem mitteilen! Das Passwort darf nur dem Nutzer bekannt sein. Mindestlänge: 6 Stellen, besser 8. Stets alphanumerisch gestalten (Buchstaben und Zahlen/Zeichen). Keine Trivialpassworte (z. B. 4711, 12345 oder andere nebeneinander liegende Tasten) verwenden. In angemessenen Zeitabständen ändern; nicht zu oft! Usw.

**Einmal-Passwort:** Beim Einmal-Passwort wird jedes Passwort nur einmal verwendet. Dabei werden grundsätzlich zwei Methoden unterschieden. Bei der ersten Methode werden Pass-

worte im Vorfeld bestimmt und verteilt. Bei der zweiten Methode berechnen die Nutzer die Passworte, nach einem definierten Verfahren, selber.

**Challenge-Response-Verfahren:** Beim Challenge-Response-Verfahren muss sich der Nutzer spontan kryptographisch beweisen. Dazu werden ein Schlüssel und ein kryptographisches Verfahren benötigt. Eine Möglichkeit ist z.B. als Challenge eine Zufallszahl zu verwenden, die dann von der SmartCard des Nutzers nach deren Aktivierung signiert wird.

**Biometrische Verfahren:** Bei Biometrischen Verfahren findet die Identifikation und Authentifikation mittels biometrischer Merkmale statt. Hier wird zwischen aktiven Verfahren, wie Stimme, Unterschrift, Gestik, Tippverhalten und passiven Verfahren, wie Fingerabdruck, Retina, Iris, Gesicht, Ohr unterschieden. Im Internet sind solche Verfahren weniger geeignet.

Zurzeit arbeiten die meisten Webanwendungen mithilfe von Passwortverfahren. Das besondere Problem bei den Passwörtern im Internet ist, dass wir für jeden Dienst eine andere Identität und ein anderes Passwort brauchen und/oder verwenden sollen. Da wir aber immer mehr Dienste im Internet nutzen, stehen wir vor der Herausforderung bis zu 50 Identitäten und Passwörter sicher verwalten zu müssen, was in der Praxis eine sehr große Schwachstelle und damit ein sehr großes Risiko darstellt, da wir meistens immer das gleiche Passwort verwenden oder diese unsicher aufschreiben.

Es gibt interessante „Identity Management Systeme“ für Internet-Dienste, wie z.B. die Liberty Alliance, die leider aber noch nicht stark genug verbreitet und in Anwendung sind. Das Ziel von Identity Management Systemen ist, vertrauenswürdige, identitätsbezogene Prozesse plattformübergreifend und standardisiert, nutzbar zu machen.

Der Aspekt Identifikation und Authentifikation ist eine sehr große Schwachstelle für alle Dienste im Internet. Nur mit Hilfe von gemeinsamen Infrastrukturen, wie z.B. die der Liberty Alliance oder PKI-basierte Authentifikationsverfahren kann dieses Problem gemeinsam gelöst werden und damit ein notwendiger und passender Sicherheitslevel erreicht werden.

## **Verschlüsselung zwischen Browsern und Webservern**

Da das Internet offen ist und die gesetzlichen Rahmenbedingungen weltweit sehr unterschiedlich sind (Asien, AUS, Europa, usw.), ist die Nutzung der Verschlüsselung für die Kommunikation zwischen Client und Server von besonderer Sicherheitsbedeutung [DiPo06]. Sehr viele Sicherheitsaspekte im Web haben mit der Einrichtung einer vertrauenswürdigen Verbindung zwischen Client und Server zu tun. Der vorherrschende Ansatz für die Verschlüsselung im Web ist die Verwendung von SSL (Secure Socket Layer).

SSL ist ein von der Firma Netscape entwickelter Verschlüsselungsstandard (Protokoll), zur sicheren Datenübertragung im Internet, welcher auf unterschiedliche Verschlüsselungs- und Authentifikationsmethoden basiert. Die verschlüsselte Kommunikation wird hierbei mittels Tunneling ermöglicht (z.B. https). Dieser Standard dient beispielsweise zum Schutz vor unberechtigtem Zugriff auf private Daten durch Dritte während der Übertragung im Internet. SSL bietet zudem die Möglichkeit, dass sich Sender und Empfänger mittels Zertifikaten gegenüber dem Anderen authentisieren können. Das SSL-Protokoll ist applikationsunabhängig und setzt logisch auf einem Transportprotokoll auf. Heute ist SSL als RFC 2246 standardisiert und wird als Transport Layer Security (kurz: TLS) bezeichnet.

SSL/TLS bündelt 3 Dienste: Authentifizierung, Verschlüsselung, Schlüsselaustausch.

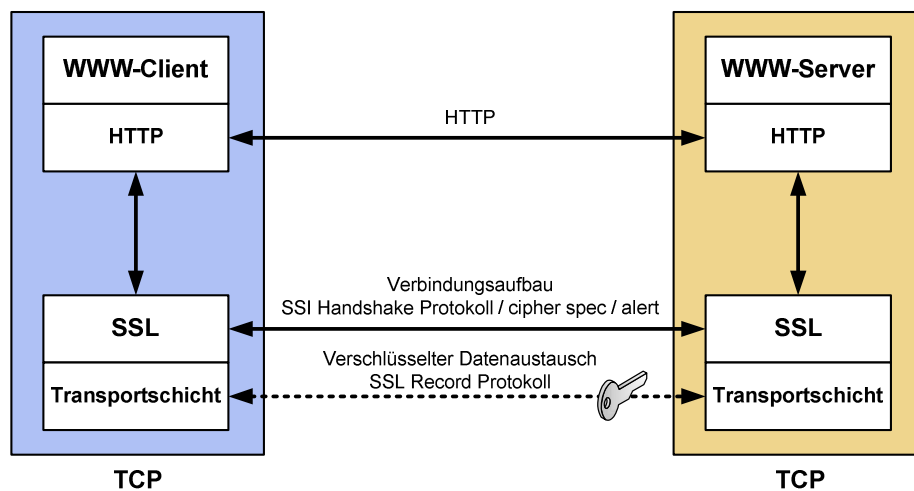


Abbildung 3: Transport Layer Security (TLS)

Die Einrichtung eines sicheren Kanals erfolgt bei SSL/TLS in zwei Phasen. Zuerst informiert der Client den Server über die kryptographischen Algorithmen, die er anwenden kann, sowie über ggf. unterstützte Komprimierungsmethoden. Die eigentliche Auswahl der kryptographischen Algorithmen bleibt dem Server überlassen, der seine Entscheidung an den Client zurückmeldet. Danach werden die Schlüssel für die Verschlüsselung ausgehandelt. In der zweiten Phase findet die Authentikation statt. Hier teilt der Server seinen öffentlichen Schlüssel dem Client durch die Übermittlung seines Domänen-Zertifikates mit. Kann der Client mit der Hilfe von Root-Zertifikaten der entsprechenden Zertifizierungsinstanzen im Browser das Domänen-Zertifikat verifizieren, so kann der Client sicher sein, dass nach einem erfolgreichen Verbindungsaufbau eine SSL-Verbindung zu genau jenem Server zustande gekommen ist, dessen Domänen-Zertifikat empfangen wurde. Nachdem die SSL-Verbindung aufgebaut ist, werden alle Anwendungsdaten in verschlüsselter Form und integ-

ritätsgesichert übertragen und wir sind uns sicher, dass wir mit dem gewollten Server kommunizieren.

## 4. Desktop-Simulationen

Im Zeitalter der Globalisierung werden Faktoren wie Mobilität und Flexibilität groß geschrieben. Daher liegt es derzeit im Trend, Softwareprogramme nicht mehr ortsgebunden daheim oder im Büro zu installieren, sondern sie mithilfe des Internets an zentralen Stellen anzubieten. Der entscheidende Vorteil: Zugriff von überall und zu jederzeit!

So genannte Desktop-Simulationen greifen diesen Aspekt auf und sind Anwendungen der modernen Art – Anwendungen auf Basis der Web 2.0 Technologie. Diese werden wie bisherige Anwendungen lokal ausgeführt, obwohl im Vorfeld keine lokale Installation, wie sonst bei Anwendungen üblich, stattgefunden hat. Die Bedienung findet einzig und allein über einen Browser mit aktiviertem JavaScript statt. Eine schnelle Anbindung ist zumeist Voraussetzung, um die Desktop-Simulationen in vertretbarer Zeit zu laden sowie die Latenzzeiten der Mensch-Computer-Interaktion möglichst gering zu halten. In Analogie zur so genannten Java Virtual Machine, die es erlaubt Computerprogramme auf Basis der Java-Technologie plattformunabhängig und somit auf nahezu jedem Betriebssystem auszuführen, kann das ebenso plattformunabhängige Web als Betriebssystem für Desktop-Simulationen verstanden werden [Pohl03]. Damit können die Anwendungen auf unterschiedlichen Plattformen, wie mobile Geräte (bspw. PDAs und Mobiltelefonen) zum Einsatz kommen, solange sie die notwendigen Anforderungen an die anwendungsabhängigen Ressourcen erfüllen. Dies vereinfacht den Umgang für den Benutzer deutlich.

Im Hinblick auf die Einführung des Web 2.0 kommen neben Online-Spielen zahlreiche, zum Teil sehr professionelle, Desktop-Simulationen auf den Markt [CrPJ06]. Diese haben gegenüber den klassischen Anwendungen besondere Vorteile aber auch Sicherheitsrisiken, die zusammen betrachtet im Folgenden umrissen werden. So muss der Nutzer von Desktop-Simulationen weder eine Software installieren noch neue Updates einspielen, um Features zu erweitern oder Sicherheitslücken zu schließen. Updates müssen nicht mehr einzeln geladen und installiert werden, sondern sind beim nächsten Start einer Desktop-Simulation bereits automatisch integriert. Aufgrund der Bequemlichkeit der Benutzer, welche aber auch oft mit dem Einspielen von Updates überfordert sind, liefert die automatische Integration von Sicherheitspatches einen entscheidenden Gewinn für die Sicherheit. Liegt ein Sicherheitsrisiko bei einer vorherigen Programmversion vor, ist es nicht mehr zwingend erforderlich den Anwender darüber zu informieren. Das heißt, durch das automatische Einspielen von Sicherheitspatches wird das Zeitfenster der Verwundbarkeit zwischen dem Erscheinen und der

manuellen Installation eines Sicherheitspatches stark minimiert. Mithilfe dieser Lösungen kann den wachsenden Mobilitätsanforderungen vieler Unternehmen nachgekommen werden.

Klassische Desktop-Applikationen, die sonst lokal geladen wurden, können als virtuelle Desktop-Anwendungen über das Internet gestartet werden [Garr05]. Sogar vollwertige, so genannte virtuelle Betriebssysteme, die ein ganzes Set an Applikationen wie Taschenrechner, Kalender, Tabellenkalkulation, Textverarbeitung und auch Grafikbearbeitung bereitstellen, gehören inzwischen nicht mehr der Vergangenheit an. Sie können mit einem ausreichend schnellen Internetzugang sowie einem Browser ein Betriebssystem von nahezu überall in Echtzeit simulieren.

Die meisten Web 2.0 Anwendungen stellen Möglichkeiten zur Verfügung, die bearbeiteten Dokumente auch online zu speichern. Praktisch dabei ist, dass keine Medien wie CDs oder USB-Sticks zum Abspeichern mehr notwendig sind. Mit der Verknüpfung persönlicher und geschäftlicher Dokumente können in Verbindung mit Web 2.0 Anwendungen individuelle Profile betrieben werden, sodass das Büro zu jeder Zeit an jedem Ort verfügbar wird. Der webweite Zugriff auf die Geschäftsdaten erlaubt es damit beispielsweise Termine zu verschieben, Artikel zu überarbeiten oder Kalkulationen durchzuführen. Aber insbesondere Anwendungsfälle dieser Art setzen die Bearbeitung von sensiblen und persönlichen Daten mit hohem materiellem Wert voraus. Doch wie sieht es mit der Sicherheit aus?

Die folgende Abbildung skizziert das Szenario einer Desktop-Simulation unter besonderer Berücksichtigung von Gefahren und Risiken in punkto Sicherheit.

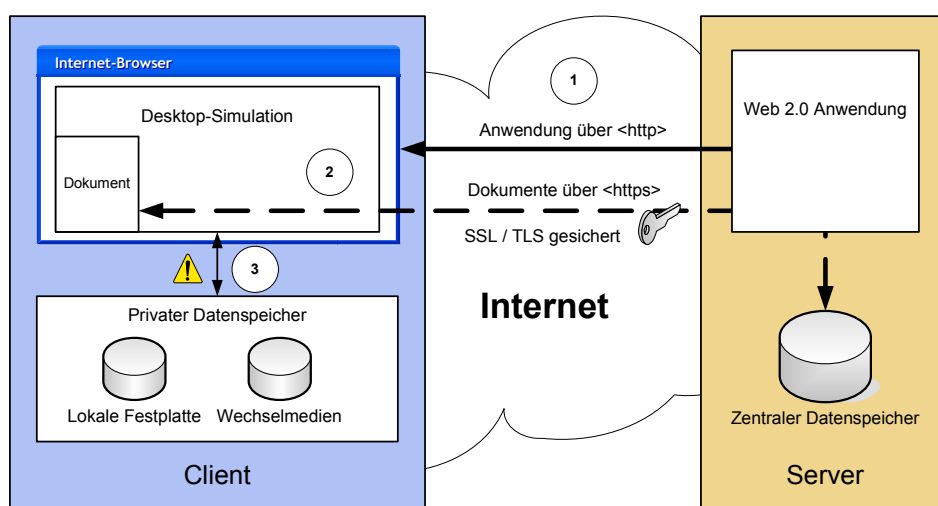


Abbildung 4: Desktop-Simulation auf Basis der Web 2.0 Technologie

Dank moderner Web-Anwendungen kann ein Anwender bestimmte Dokumente auch ohne lokale Installation einer speziellen Software bearbeiten. Dazu können durch Aufruf einer

Web 2.0 Anwendung, je nach Art des zu bearbeitenden Dokuments, unterschiedliche Desktop-Simulationen über einen Internetbrowser aufgerufen werden (vgl. Schritt 1 in Abbildung 2). Da bei diesem Vorgang keine vertraulichen Daten übertragen werden, ist eine verschlüsselte Verbindung nicht erforderlich. Werden hingegen neben der Übertragung einer Anwendung auch persönliche Profile und somit vertrauliche Daten geladen oder gespeichert, ist eine verschlüsselte Verbindung unumgänglich. Dafür ist es notwendig, dass sich der Nutzer gegenüber dem Anbieter über eine gesicherte Verbindung authentisiert.

Wenn nach erfolgreicher Authentikation der Zugriff auf die Profildaten freigegeben wurde, ist es genauso wichtig, dass die Daten beim Empfang und Versand verschlüsselt übertragen werden. Sonst besteht die Gefahr, dass die Daten während der Übertragung unbemerkt von unautorisierten Personen mitgelesen werden.

Abgesehen von diesen Sicherheitsmechanismen muss stets hinterfragt werden, ob der Dienstanbieter von Web 2.0 Anwendungen auch vertrauenswürdig ist. Hat der Anbieter Zugriff auf individuelle Profildaten seiner Kunden, weil sie nicht verschlüsselt hinterlegt werden? Kann der Nutzer der herunter geladenen Software des Dienstanbieters vertrauen oder muss er befürchten, dass mittels ungewollter Zugriffe auf seine lokalen Daten auch privaten Daten unbewusst über die Desktop-Simulation zum Anbieter gelangen? (vgl. Abbildung 2, Schritt 3)

Es wird daher empfohlen, einen Dienstanbieter für Desktop-Simulationen auszuwählen, welcher als vertrauenswürdige Instanz eingestuft worden ist und ausreichend vor Bedrohungen von außen, aber auch gegen Spionage von innen geschützt ist. So sollten insbesondere sensible Daten nicht im Klartext, sondern verschlüsselt gespeichert werden.

Um die Integrität der Daten zu gewährleisten, sollte neben der Datenverschlüsselung ein digitaler Fingerabdruck (Hash-Wert) generiert werden. Damit hat der Nutzer beim zukünftigen Laden seines Profils die Möglichkeit, die Daten auf Manipulation zu überprüfen (Fingerprint-Vergleich).

Insbesondere die Verfügbarkeit eines Dienstanbieters darf nicht vernachlässigt werden. Damit Dienste für Web 2.0 Technologien zur Verfügung stehen, sind jedoch zwei Szenarios denkbar.

- a) Um eine möglichst hohe Verfügbarkeit zu erzielen, können zum einen mittelständische bis große Unternehmen, bei denen eine Anschaffung einer unternehmenseigenen Web 2.0 Infrastruktur den Kosten angemessen ist, die Dienste der Web 2.0 Technologie ihren Mitarbeitern aus dem Unternehmen heraus anbieten. Dies ermöglicht zum Beispiel eine zentrale Backup-Strategie und damit eine deutliche Verbesse-

rung der Verfügbarkeit der Daten sowie auch, falls der Schutzbedarf dies erfordert, eine Verbesserung der Anwendungsverfügbarkeit mittels redundanter Lösungen.

- b) Das zweite Szenario ergibt sich durch die Anmietung der Dienstleistung des Anbieters oder durch eine zumeist kostenlose Nutzung für private Personen. Bei diesem Szenario ist auf der einen Seite wichtig zu wissen, in welchem Maße eine Verfügbarkeit der Daten gegeben ist. Sind die Daten bei einem Konkurs des Anbieters nicht verloren? Dies ergibt sich zumeist aus den AGBs der Anbieter. Auf der anderen Seite sollte auf eine ausreichend gute Verfügbarkeit der Web 2.0 Anwendungen geachtet werden. Das ist notwendig, damit Dokumente die mit speziellen Anwendungen erstellt worden sind, jederzeit bearbeitet werden können. Um beispielsweise beim Serverausfall eines Anbieters dennoch unabhängig von diesem weiterarbeiten zu können, ist es sinnvoll solche Anwendungen auszuwählen, die bei verschiedenen Anbietern angeboten werden. Die Verfügbarkeit von Web 2.0 Diensten für Desktop-Simulationen lässt sich noch weiter verbessern, wenn sich Dokumente nicht nur mit speziellen Anwendungen bearbeiten lassen. Es wäre daher angemessen, die Dokumente in einem standardisierten, generischen oder offenem Format zu speichern, damit sie mit verschiedenen Anbieterlösungen oder auch mit lokalen Anwendungen bearbeitet werden können.

Web 2.0 kann die Produktivität und die Wertschöpfung steigern, führt jedoch auch zu einem erhöhten Management- und Sicherheitsaufwand für die IT-Abteilung eines Unternehmens. Es sollte stets überlegt werden, ob sich der Preis für Flexibilität und Mobilität bezahlbar macht. Auf der einen Seite können durch die Verwendung der neuen Technologie sicherlich viel Zeit und Kosten eingespart werden, weil die Daten jederzeit – unter Berücksichtigung der Verfügbarkeit – und von nahezu überall abgerufen werden können. Auf der anderen Seite muss auch der größte anzunehmende Schaden berücksichtigt werden, indem beispielsweise Konkurrenzunternehmen unbemerkten Zugriff auf hochsensible Daten erhalten.

Es wird daher zunächst empfohlen, keine sensiblen Daten über Web 2.0 Desktop-Simulationen auf Online-Speichern von Dienstleistern zu hinterlegen. Auch die Bearbeitung mit solchen Programmen ist derzeit noch zu riskant. Die Anbieter müssen erst von Zertifizierungsdienstleistern, wie TÜVs, evaluiert und zu vertrauenswürdigen Anbietern ernannt werden. Sonst könnten nicht zertifizierte Anwendungen schädlichen Code ausführen und auf lokal gespeicherte Daten, beispielsweise durch vorhandene Sicherheitslücken, Zugriff erhalten (vgl. Abbildung 2, Schritt 3). Diese Daten könnten daraufhin unbemerkt zum Anbieter übertragen werden. Es ist nicht praktikabel und für einen normalen Benutzer zudem nicht durchführbar ständig zu überprüfen, welche Daten tatsächlich an den Anbieter einer Web 2.0 Anwendung übertragen werden (beispielsweise lokale Daten seiner Festplatte). Desktop-

Simulationen sollten daher von Zertifizierungsdienstleistern digital signiert werden, sodass der Anwender diese nach dem Ladevorgang auf Echtheit überprüfen kann.

## 5. Basissicherheit für Anbieter von Webanwendungen

Die Anbieter von Webanwendungen sollten für ihre Infrastruktur ein gehärtetes Betriebssystem, das heißt ein Betriebssystem verwenden, welches nur essentielle Funktionen bereitstellt. Denn durch die Minimalisierung des Funktionsumfangs ist die Fehlerwahrscheinlichkeit wesentlich geringer und die Vertrauenswürdigkeit höher. Darüber hinaus ist das Betriebssystem insbesondere vor Angriffen von außen durch den Einsatz von Firewalls, Sicherheitspatches und aktuellen Virensclannern optimal zu schützen.

Neben sicheren Betriebssystemen mit entsprechender Hardware sollten auch die Webanwendungen sicher konfiguriert sein. Sowohl die Dienste, als auch eventuell zugrunde liegende Content-Management-Systeme oder andere eingesetzte Open-Source-Produkte sollten sich auf dem neuesten Stand befinden. Dies vermindert die Chance auf erfolgreiche Angriffe, welche nach Veröffentlichungen von Sicherheitslücken vermehrt auftreten. Außerdem sollten die Entwickler von Web 2.0 Anwendungen Sicherheitsaspekte bei der Entwicklung berücksichtigen, sowie bei der Implementierung eine Technologie verwenden, die für eine sichere Anwendung ausgelegt ist.

Auf die Gewährleistung der Verfügbarkeit sollte mit einem Redundanzkonzept eingegangen werden, welches die Ängste der Nutzer vor Datenverlust oder Verfügbarkeitsprobleme minimiert.

Anbieter von Web 2.0 Technologien, welche persönliche, geschäftliche und somit zumeist auch Daten von hohem materiellem Wert verwalten, sollten sich von Zertifizierungsdienstleistern zu vertrauenswürdigen Anbietern ernennen lassen.

## 6. Tipps im Umgang mit Web 2.0 für den Benutzer

- **Vertraulichkeit**

Um generell eine hohe Vertraulichkeit beim Umgang mit Web 2.0 Anwendungen zu erzielen, sollten einerseits die Anwendungen und Dienste und andererseits die Online-Speicher für sensible Daten von Zertifizierungsdienstleistern geprüft werden. Außerdem sollten sensible Daten mithilfe eines Schlüssels (wie Passwort oder Zertifikat) gesichert werden (vgl. Groupwaredienste im Internet).

- **Authentikation**

Im größtenteils anonymen Internet sollte dem Kommunikationspartner nicht blind vertraut werden, da nicht sichergestellt ist, ob dieser wirklich der ist, für den er sich ausgibt. Dies gilt sowohl für Kontakte innerhalb von „Social Networks“, als auch für die Dienstanbieter selbst.

- **Integrität**

Um die Integrität persönlicher Daten auf Online-Speicher zu gewährleisten, sollten diese mit einem digitalen Fingerabdruck (Hash-Wert) versehen werden. Dieser lässt sich auf Basis der Datenmenge nahezu eindeutig und relativ einfach errechnen. Hat sich der Hash-Wert und somit der digitale Fingerabdruck ohne Kenntnis des Eigentümers verändert, ist dies ein Indikator dafür, dass die Daten manipuliert worden sind.

- **Verfügbarkeit**

Um eine möglichst permanente Verfügbarkeit der Daten zu gewährleisten, welche unter Umständen bei einer Providerstörung nicht gegeben ist oder bei einem Konkurs des Dienstanbieters im ungünstigsten Fall zu einem vollständigen Datenverlust führt, wird empfohlen, regelmäßig lokale Backups zu erstellen.

- **Informationelle Selbstbestimmung**

Zum Schutz personenbezogener Daten sollten die AGBs des Dienstleisters vor deren Preisgabe geprüft werden. Zu beachten ist hierbei, ob Daten an Dritte weitergegeben werden und besonders in welchem Ausmaße.

Wie der Artikel gezeigt hat, birgt Web 2.0 neben neuen Möglichkeiten und vielerlei Vorteilen eine Menge an Gefahren und Risiken. Um viele der Probleme von Grund auf zu minimieren, ist es eine strukturierte Herangehensweise eine vertrauenswürdige Ausführungsumgebung zu schaffen. Von dieser Plattform aus kann dann eine vertrauenswürdige Kette geschaffen werden, die bei der Hardware des Dienstanbieters beginnt, sich über Übertragungsleitungen fortsetzt und letztendlich bei der Anwendung des Nutzers endet. Dieser Aspekt wird im folgenden Abschnitt näher erläutert.

## 7. Ausblick

Damit die größten Sicherheitsprobleme im Internet gelöst werden können, wird eine **Sicherheitsplattform** für Rechnersysteme benötigt, die auf **Trusted Computing** basiert.

Trusted Computing ist eine Sicherheitstechnologie, die von einem Industriekonsortium mit über 170 internationalen Mitgliedern entwickelt wird (siehe [www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org)). Die Ergebnisse dieses Konsortiums sind offene Spezifikationen, die grundsätzlich das Ziel haben, IT-Systeme vertrauenswürdiger zu machen. Die Spezifikation des Trusted Platform Module's (kurz: TPM), ein manipulationssicheres Sicherheitsmodul für Rechnersysteme, ist von vielen Herstellern umgesetzt worden und derzeit in bereits über 60 Millionen Rechnersystemen integriert.

Dieses Sicherheitsmodul wirkt als vertrauenswürdiger Anker in einem Rechnersystem (Root of Trust), indem mittels Hashfunktionen die Systemkonfiguration des Rechnersystems komplett gemessen wird und damit später überprüfbar ist. Für Web 2.0 Anwendungen bedeutet das, dass einzelne Anwender überprüfen können, ob sich ein Server- und Clientsystem in einer Systemkonfiguration befindet, die als sicher einzuschätzen ist.

Das Forschungs- und Entwicklungsprojekt EMSCB (European Multilaterally Secure Computing Base) [PSS04], an dem mehrere Hochschulen und IT-Sicherheitsfirmen beteiligt sind, stellt mit Turaya eine vertrauenswürdige, faire und offene Sicherheitsplattform zur Verfügung, die auf Trusted-Computing-Technologie aufbaut (vgl. [www.emscb.org](http://www.emscb.org)).

Ziele des Projektes sind: Eine Sicherheitsplattform mit offener Architektur und Schnittstellen zu schaffen, die als Basis für vertrauenswürdige IT-Systeme dient. Durch die Bereitstellung der Sicherheitsplattform für PCs, PDAs, Mobiltelefone und embedded systems werden neue, innovative Geschäftsmodelle ermöglicht. Die **Sicherheitsplattform** Turaya ist ein betriebssystem-ähnlicher Sicherheitskern, der auf einem Mikrokern basierend aus einer sehr geringen Codebasis besteht und daher weit weniger komplex ist, als etablierte Betriebssysteme. Durch diese Minimalisierung ist die Fehlerwahrscheinlichkeit wesentlich geringer bei deutlich größerer Vertrauenswürdigkeit. Mit Turaya ist es möglich, einzelne sichere Applikationen vollständig isoliert, in so genannten Compartments, vom etablierten Betriebssystem parallel auszuführen. Die Vertrauenswürdigkeit der sicheren Applikationen (Secure Application) wird durch die Messmöglichkeit des TPMs (Trusted Computing Hardware) überprüfbar gemacht. Das etablierte Betriebssystem kann demnach durch Malware kompromittiert worden sein, da alle sicherheitskritischen Vorgänge außerhalb des Betriebssystems von sicheren Anwendungen ausgeführt werden können.

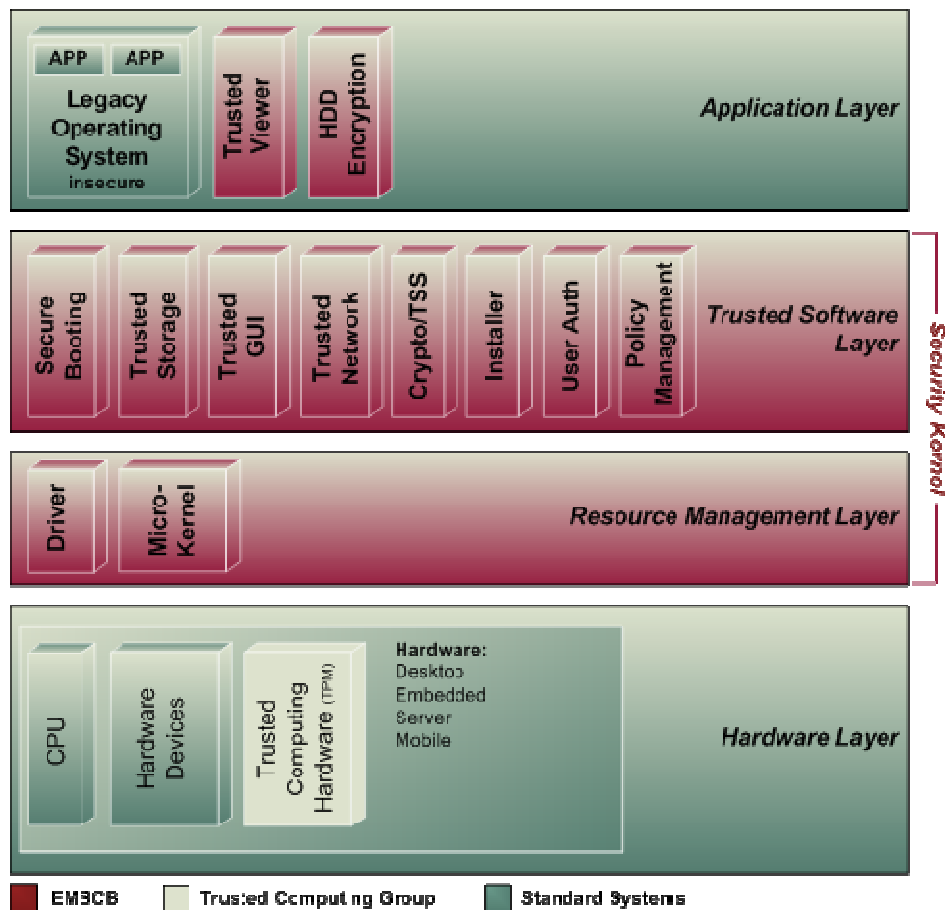


Abbildung 5: Turaya Architektur

Die Sicherheitsplattform Turaya in Kombination mit der Trusted Computing Technologie bietet ein breites Spektrum an Gestaltungsmöglichkeiten von vertrauenswürdigen Anwendungen, welche auch bei der Web 2.0 Technologie erforderlich sind. Schadsoftware, wie z.B. Trojanische Pferde und Viren werden schlicht von sicherheitsrelevanten Daten isoliert. Server und Clientsysteme können zuverlässig authentifiziert werden [LiPo06]. In diesem Projekt wird weltweit die erste Sicherheitsplattform entwickelt, die auf Trusted Computing aufbaut und somit eine viel versprechende Verbesserung der Sicherheit für zukünftige Rechnersysteme darstellt. Erste größere Projekte mit SAP, Banken und Content-Providern zeigen die Notwendigkeit für den Markt auf.

## Literatur

- [Pohl02a] N. Pohlmann: "Die Welt ist nicht perfekt", Sicherheit + Management – Magazin für Safety und Security, GIT Verlag, 5/2002
- [DOS03] M.C. Daconta, L.J. Oberst, K.T. Smith: „The Semantic Web: A Guide to the Future of

- 
- XML, Web Services and Knowledge Management“, Wiley Publishing, Indianapolis, 2003
- [HePo06] M. Hesse, N. Pohlmann: „Trickbetrügern auf der Spur: Wie man der Phishing-Welle entkommen kann“, Bankinformation und Genossenschaftsforum, Deutscher Genossenschafts-Verlag, Wiesbaden, 1/2006
- [Pohl03] N. Pohlmann: "Firewall-Systeme-Sicherheit für Internet und Intranet, E-Mail-Security, Virtual Private Network, Intrusion Detection-System", MITP-Verlag, Bonn 2003
- [CrPJ06] D. Crane, E. Pascarello, D. James: „Ajax in Action. Das Entwicklerbuch für das Web 2.0“, Addison-Wesley, 8/2006
- [Garr05] J. Garrett: „Ajax: A New Approach to Web Applications“, Adaptive Path LLC, 2/2005
- [PSS04] N. Pohlmann, A.-R. Sadeghi, C. Stüble: "European Multilateral Secure Computing Base", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 09/2004
- [LiPo06] M. Linnemann, N. Pohlmann: „Die vertrauenswürdige Sicherheitsplattform Turaya“, in "DACH Security 2006", Hrsg.: Patrick Horster, syssec Verlag, 2006