

Kaufmännische Mietsoftware, eigene Server und die Sicherheit.

Netzwerk Elektronischer Geschäftsverkehr (NEG)

Mainfränkisches ECommerce Kompetenzzentrum (MECK)

Begleitvorhaben ERP am Lehrstuhl für BWL und Wirtschaftsinformatik der Universität Würzburg (Prof. Thome)

erp@wiinf.uni-wuerzburg.de

<http://www.meck-online.de>

<http://www.ec-net.de>

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 28 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business-Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

1 Ist die Zeit reif für Mietsoftware über das Internet?

Zurzeit lässt sich ein Trend namens SaaS (Software-as-a-Service) beobachten. Im Wesentlichen handelt es sich hierbei um die Idee, Software auf den Systemen eines Drittanbieters gegen Entgelt (Miete) zu nutzen, anstatt sie auf den betriebseigenen Computern (Servern) zu installieren. Um diese Dienstleistung nutzen zu können, muss der Nachfrager (ihr Unternehmen) über das Internet mit den Systemen des Anbieters verbunden sein. Die Idee der Softwaremiete erfreut sich wachsender Beliebtheit. Dieses Dokument des Netzwerks Elektronischer Geschäftsverkehr (NEG, <http://www.ec-net.de>) vergleicht Mietsoftwarelösungen mit traditionellen Lösungen, unter dem Hauptaspekt der Informationssicherheit und ist auf kaufmännische Softwarelösungen bzw. Enterprise-Resource-Planning-Lösungen (ERP) fokussiert.

2 Kaufmännische Software und ERP

Bei kaufmännischer Software bzw. ERP (wird ab hier synonym verwendet) handelt es sich im Allgemeinen um Software, die zur betrieblichen Leistungserstellung in und zwischen Unternehmen eingesetzt wird.

2.1 Inhouse-ERP

ERP-Systeme kombinieren alle benötigten Bereiche zur betrieblichen Leistungserstellung entlang der Wertschöpfungskette im Unternehmen. Dazu gehören alle Grundfunktionen, wie Beschaffung und Vertrieb, und Querschnittsfunktionen, wie Personal- und Finanzverwaltung. Neben branchenneutralen Anwendungen umfasst ERP-Software auch branchenspezifische Lösungen.

Als physische Grundlage für ERP-Systeme hat sich Ende der 90er Jahre der Client-Server-Ansatz etabliert: Die Clients bedienen sich dabei Funktionen der Server. Die Server-Funktionen sind dabei aufgeteilt in Präsentation, Anwendung und Datenbank und laufen auf separaten Rechnern. Dadurch ist es möglich, die Rechenlast nicht nur auf einen Computer, sondern über ein Netzwerk zu verteilen, und das bei zentraler Datenablage und integrierter Datennutzung. Befindet sich der Server nun in den Räumen ihres Unternehmens, so spricht man von einem Inhouse-ERP-System.

2.2 SaaS-Konzept

Bei Software als Dienstleistung, im Gegensatz zur Software als Produkt, liegt letztendlich dieselbe Konstruktion wie beim Inhouse-ERP zugrunde, nur dass sich das Server-System nicht im Unternehmen, sondern bei einem Dienstleister befindet und diesem auch eigentumsrechtlich gehört. Bildlich kann man sich das so vorstellen, dass die Netzkabel der Serversysteme über das Internet verlängert werden, was zu einer räumlich Verschiebung und administrativen Neuverantwortlichkeit der Serverrechner führt. Der SaaS-Anbieter (Dienstleister) stellt dem SaaS-Nachfrager (ihr Unternehmen) die Nutzung seiner Systeme gegen ein fixes, variables, monatliches, jährliches oder leistungsbezogenes Entgelt zur Verfügung. Der SaaS-Nutzer bezieht diese Leistung über ein Netz, das in den meisten Fällen das Internet, also öffentlich, ist. Der SaaS-Nutzer hat den Vorteil, dass der Anbieter die Kosten für die Anschaffung, den Betrieb und die Verantwortung für die Sicherheit trägt und sich um die Wartung der Server kümmert.

3 Gemeinsamkeiten der Sicherheitsproblematik

Um die Inhouse- und die SaaS-Lösung anhand von Sicherheitsaspekten vergleichen zu können, erfolgt zunächst eine Herausarbeitung der gemeinsamen Sicherheitsprobleme.

3.1 Schutzziele

Nach ISO/IEC 27001 gibt es im Sinne der Informationssicherheit vor allem drei international anerkannte Sachziele: Vertraulichkeit, Integrität und Verfügbarkeit. Unter Vertraulichkeit versteht man, dass die entsprechenden Daten nur berechtigten Personen zugänglich gemacht werden. Integer sind Daten in einem Unternehmen dann, wenn ausschließlich autorisierte und beabsichtigte Veränderungen vorgenommen wurden, d. h. keine ungewollten Verfälschungen oder gezielte Manipulationen der Daten vorliegen. Als Verfügbarkeit ist die Fähigkeit eines IT-Systems definiert, Daten in bestimmter Form und Qualität innerhalb nützlicher Frist bereitzustellen.

3.2 Bedrohungen und Schwachstellen

Durch Schwachstellen in der IT-Landschaft eines Unternehmens können Bedrohungen und Gefahren für Daten und Unternehmen entstehen. Zuerst sucht man nach möglichen Bedrohungen und über welche Schwachstellen diese wirken können, um einen wirksamen Schutz aufbauen zu können.

Natürliche Schwachstellen ergeben sich aus dem Umstand, dass Computersysteme für Naturkatastrophen, wie Feuer, Hochwasser, Blitzschlag, und andere Umwelteinflüsse, wie Staub oder hohe Luftfeuchtigkeit, anfällig sind.

Gebäude und Computerräume können physische Schwachstellen aufweisen. Gebäude sind beispielsweise anfällig für Einbrüche. Medien (USB-Stick, CDs) sind anfällig für Beschädigungen oder Diebstahl.

Technische Schwachstellen entstehen bei Hard- und Software durch unsachgemäße Benutzung, beispielsweise durch Überlastung oder falsche Verschaltung oder durch konzeptionelle Fehler oder Programmierfehler.

Darüber hinaus ist nicht zuletzt der Mensch als Administrator oder Benutzer eine Schwachstelle für Computersysteme.

Ein weiteres Risiko sind Kommunikationsleitungen, die zur Vernetzung von Computern untereinander dienen, da diese abgehört und beschädigt werden können oder ausfallen.

Es wird zwischen beabsichtigten und unbeabsichtigten Bedrohungen und höhere Gewalt unterschieden. Hierzu gibt es viele Vorgaben und Materialien des Bundesamtes für Sicherheit in der Informationstechnik (BSI, <http://www.bsi.de>). Zu den unbeabsichtigten Bedrohungen zählen Unwissenheit, Unaufmerksamkeit oder das Außerachtlassen von Sicherheitsaspekten. Ein Beispiel dafür ist der Verlust eines Speichermediums.

Beabsichtigte Bedrohungen können von innen oder von außen kommen. Zu den potentiellen außenstehenden Angreifern gehören Geheimdienste, Terroristen, Konkurrenzfirmen oder Cracker. Externe Angreifer können auf vielfältigen Wegen in ein System eindringen: Physischer Einbruch, Missbrauch sozialer Kontakte, als Wartungs- oder Service Personal verkleidet, über Spoofing, Phishing, Sniffing oder mit Hilfe von Computerviren, Trojanern und Würmern. Angriffe von Insidern sind ebenfalls auf verschiedene Arten möglich: Ein entlassener oder unzufriedener Mitarbeiter kann seine Zugriffsprivilegien verwenden, um nicht autorisierte Funkti-

onen auszuführen, Informationen aus dem Unternehmen zu schleusen oder anderweitig Wissen zu seinem Vorteil zu nutzen, oder um einfach die tägliche Arbeit stören.

3.3 Gegenmaßnahmen

IT-Sicherheit ist, laut BSI, als der Zustand eines IT-Systems definiert, „in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind“. (Quelle: Bundesamt für Sicherheit in der Informationstechnik).

3.3.1 Physische Sicherheit

Die physische Sicherheit ist der Schutz von Computersystemen gegen Schäden durch natürliche Bedrohungen und Einbrecher. Schutz dagegen bieten neben einer soliden Bauweise von Gebäuden und Räumen auch technische Anlagen, wie Klimaanlage, Feuermelde- und Feuerlöschsysteme und unterbrechungsfreie Stromversorgungen (USVs) mit Überspannungsschutz. Schutz gegen Zutritt unbefugter bieten mechanische Schlösser oder moderne Zutrittskontrollsysteme. Ferner können Alarmanlagen und Videoüberwachungssysteme bzw., in Sektoren mit besonders sensiblen Daten, wärme-, druck- oder bewegungsempfindliche Sensoren eingesetzt werden.

Server der Mietsoftwareanbieter sind in einem Rechenzentrum physisch besser geschützt als Server in einem Raum in ihrem Unternehmen.

3.3.2 Computersicherheit

Computersicherheit bedeutet Schutz der **Informationen**, die in einem Computersystem gespeichert sind, und nicht den Schutz des Gerätes selbst. Der Sicherheitsaspekt sollte sich demnach auf die Funktionalität des IT-Systems konzentrieren, über das Systemzugriffe und die Bearbeitung der Daten kontrolliert werden (Betriebssystemsicherheit). Wichtig ist aber auch die Sicherheit von Datenbanken und Anwendungsprogrammen. Dazu gehören sichere Benutzernamen und Passwörter, differenzierte Benutzerrechte, Protokolle zur Nachverfolgung und Auswertung, administrative Vorgänge (wie das Erstellen von Sicherungskopien) und das regelmäßigen Einspielen von Updates und Sicherheits-Patches.

Das Einspielen von Patches und die Aktualisierung der Serverbetriebssysteme wird bei Mietsoftware an den Dienstleister abgegeben. Dennoch bleibt viel Verantwortung bei den Geschäftsführern, den Systemverantwortlichen und auch bei jedem einzelnen Benutzer (etwa Passwörter)

4 Unterschiede in der Sicherheitsproblematik

Die Tatsachen, dass Daten nicht im eigenen Haus gespeichert werden und über ein öffentliches Netz übertragen werden, stellen neue Herausforderungen an die Sicherheit.

4.1 Kommunikations- und Datensicherheit

Allgemein ist Kommunikationssicherheit der Schutz von Daten während der Übertragung mittels Telekommunikationseinrichtungen.

Benutzer von Mietsoftware haben nur noch begrenzt Kontrolle über die Kommunikationseinrichtungen (Server und Internet). Regelungen über die Verfügbarkeit der Informationssysteme des beauftragten SaaS-Anbieters müssen daher durch sogenannte Service-Level-Agreements (SLA) vereinbart werden. Das sind schuldrechtliche Verträge, die eine Vielzahl von rechtlich verbindlichen Absprachen treffen, z. B. Verfügbarkeitsquoten des Systems. Auch wenn oft argumentiert wird, dass SaaS-Nutzer von einer hohen Verfügbarkeit profitieren, so sind die getroffenen Vereinbarungen doch extrem genau zu prüfen.

Eine Serviceverfügbarkeit von 99% klingt sehr hoch. Bei 365 Tagen im Jahr dürfte ein System aber fast vier Tage ausfallen! Daher sind die Nachkommastellen hier wichtig: Bei 99,99% sind es nur noch wenige Stunden.

4.2 Datenschutz

Datenschutz umfasst zum einen die Sicherheit der Datenverarbeitungssysteme, wie in den vorigen Kapiteln beschrieben (§9 sowie Anlage zu §9 BDSG), und zum anderen die Regularien, die der Datenverarbeitung zugrunde liegen. Beim Software-Outsourcing (Miete!) wird laut Bundesdatenschutzgesetz (BDSG) der Datenschutz erst dann relevant, wenn es sich um personenbezogene Daten handelt (§3 Abs.1 BDSG). Zu keiner Anwendung kommt es bei hinreichender Anonymisierung bzw. Pseudonymisierung der Daten (§3 Abs.6, 6a BDSG). Das kann durch Ersetzen von personenbezogenen Merkmalen erreicht werden. Bei kaufmännischer Software werden aber persönliche Daten verarbeitet und gespeichert, v.a. im Bereich des Kundenbeziehungsmanagements (CRM). Viele SaaS-Anbieter versichern, dass ihre Systeme durch aktuelle Verschlüsselungstechnologien geschützt sind, Unbefugte also nicht an die Daten gelangen können.

Das Recht auf Datenschutz ist geografisch an den Datenverarbeitungsort gebunden. Was passiert, wenn der SaaS-Anbieter im Ausland ansässig ist oder aus wirtschaftlichen Gründen Daten dort speichert?

Für Länder wie die Schweiz, Kanada oder Argentinien hat die EU-Kommission festgestellt, dass ein angemessenes Datenschutzniveau besteht. Was ist jedoch mit Ländern, in denen diese Standards nicht gelten? Auch in „westlichen“, demokratischen Staaten gibt es Probleme mit den EU-Datenschutzrichtlinien. Nur auf Basis der „Safe Harbour“-Datenschutzvereinbarung ist es weiterhin legal möglich, Daten in die USA und mit US-Unternehmen auszutauschen.

Nach Art. 2c S.1 Europäischer Datenschutzrichtlinie (EU-Datenschutzrichtlinie) ist der Nutzer (das mietende Unternehmen und dessen Verantwortliche) von SaaS für die eingesetzten Mittel und Zwecke der Datenverarbeitung verantwortlich.

Namhafte ERP-Mietsoftwareanbieter haben ihre Rechenzentren in Deutschland oder Europa. Dadurch kann davon ausgegangen werden, dass Datenschutz und Datensicherheit entsprechend den Regularien gewährleistet sind. Nichts destotrotz bleibt der Nutzer (ihr Unternehmen) für die Kontrolle der Einhaltung der Richtlinien verantwortlich.

Unter anderem in der Auftragsdatenverarbeitung nach § 11 BDSG sind die Tatbestandsmerkmale und Rechtsfolgen niedergeschrieben. Eine verbindliche und abschließende Information ist in diesem Artikel nicht möglich. Weiterführende Informationen finden Sie beim Begleitvorhaben „Netz- und Informationssicherheit“ des NEG (<http://www.ec-net.de/EC-Net/Navigation/Themen/netz-informationssicherheit.html>).

5 SaaS oder Inhouse-ERP-System

Eine Zusammenfassung der zuvor erörterten Sicherheitsprobleme und ein Versuch einen Anhaltspunkt zu geben, für welche Unternehmen kaufmännische Mietlösungen geeignet sind.

5.1 Einrichtung

Software ist im Allgemeinen sehr komplex. Bei der Einführung einer Inhouse-ERP-Lösung müssen die benötigte Hard- und Software und Sicherheitsmaßnahmen eingerichtet werden. Dieser Vorgang verursacht relativ hohe Kosten und ist für kleine und mittelständische Unternehmen (KMU) ein immenser Aufwand. Durch eine Mietlösung kann auf die teure IT-Infrastruktur verzichtet und dennoch von hohen Sicherheitsstandards profitiert werden, da die Mietsoftwareanbieter spezialisierte Rechenzentren unterhalten. Im Prinzip ist oft ein aktueller Webbrowser alles, was für eine moderne SaaS-Lösung benötigt wird. Durch die leichte Einrichtung und Bedienbarkeit wird nicht nur eine Konzentration auf die Kernkompetenzen eines Unternehmens möglich, sondern das Risiko von Fehlern bei der Einrichtung der Anwendung wird deutlich verringert. Das Geschäftsmodell der Softwaremiete ist insbesondere bei stark standardisierbaren Funktionen und Prozessen, wie bei der ERP-Software, vorteilhaft. Daher eignet es sich vor allem für KMU, die im Vergleich zu Großunternehmen ein geringeres IT-Know-how und knappere Ressourcen aller Art besitzen.

Die Einrichtung der Softwarelösung wird oft durch Branchenvorlagen erleichtert. Individualisierungen sind in begrenzten Rahmen möglich. Die Einführungszeit verkürzt sich im Vergleich zu Inhouse-Systemen.

5.2 Nutzung

Die Pflege und Wartung hausinterner ERP-Software benötigt materielle, finanzielle und personelle Ressourcen. Bei SaaS können laufende Kosten für Personal, Fortbildungen und technische Wartung (teilweise) ausgelagert werden.

Gleichzeitig profitierten die Nutzer von einer immer aktuellen Software. Bei selbst betriebenen Servern muss ein Wartungsintervall geschaffen werden und eigene Mitarbeiter müssen die Server warten. Durch die SLAs bei der Softwaremiete wird ein Großteil der Verantwortung

an den Auftragnehmer, den SaaS-Anbieter, abgegeben, der dafür verantwortlich zeichnet, dass seine Systeme frei von größeren Störungen und Fehlern funktionieren.

Um aber zumindest datenschutzrechtlich sicher dazustehen, müssen SaaS-Nutzer besonders auf die vom Dienstleister getroffenen organisatorischen und technischen Maßnahmen achten. Der Anbieter muss ein dokumentiertes Datenschutz-, Sicherheits- und Vorfalls-Management betreiben und die Datentrennungsmethoden auf den mehrmandantenfähigen Servern offenlegen. Internationale Normen sind derzeit jedoch noch nicht weit genug verbreitet (etwa der Einsatz der ISO-Norm).

Bei einer Mietlösung werden die Server vom Betreiber gewartet. Um die Clients muss ein Unternehmen sich weiterhin selbst kümmern, viele Unternehmen bedienen sich hier eines Dienstleisters. Bei einer Störung ist aber nicht immer sofort klar wo die Ursache liegt. Dies führt zu Streitigkeiten um die Zuständigkeit. Eventuell basiert eine Störung auch auf dem Ausfall der Internetverbindung. Das wäre dann in der Zuständigkeit eines Dritten Dienstleisters. Hier ist es sinnvoll eine fachkundige Person im Unternehmen zu haben, die schnell erkennt, woher technische Probleme rühren.

6 Und nun?

Mietsoftware ist eine moderne Ausprägung von Software, die neue Möglichkeiten für Anbieter und Nutzer bietet. Aufgrund der Überallverfügbarkeit bietet eine über das Internet verfügbare Arbeitsumgebung (in diesem Fall die kaufmännische Software eines Unternehmens) viele neue Möglichkeiten und erweiterten Komfort. Der Architektur der Übertragung über das Internet ist aber auch eine große Schwachstelle geschuldet: Die Daten sind theoretisch für jedermann zu erreichen. Verschlüsselung, Passwörter, Firewalls und weitere Sicherheitsmechanismen müssen sicher greifen.

Wichtig ist, dass man für sein Unternehmen eine akzeptable Mischung aus Sicherheit und Komfort findet und dann auch wirklich alle Sicherheitsmechanismen effektiv und am besten auch effizient nutzt.

Bei dem aktuellen Hype um „Cloud-Computing“ möchte man fast glauben, dass es bald keine andere Architektur mehr geben wird. Mit Sicherheit werden aber auch die altbekannten Systeme (Inhouse-Systeme) weiterhin ihre Berechtigung haben und somit eine Nachfrage am Softwaremarkt erzeugen.

Neben der Frage nach der passendsten Softwarelösung muss nun auch noch die Frage nach der Architektur beantwortet werden? Wenn man auf diese Frage zuerst eingeht, kann man das Angebot an Systemen schnell reduzieren. Vor- und Nachteile haben beide Lösungen, es kommt wieder einmal auf die gestellten Anforderungen an. Es ist also wichtiger denn je ein geeignetes Anforderungsprofil für Ihre betriebswirtschaftliche Anwendungssoftware zu erstellen.

Betriebswirtschaftliche Gründe können auch die Entscheidung für oder gegen Mietsoftware beeinflussen, denn gemietete Software darf in der Bilanz nicht aktiviert werden und stellt somit keinen buchhalterischen Sachwert dar. Umgekehrt muss gekaufte Software (ab einem bestimmten Wert) aktiviert werden. Somit kann auch durch die Softwareauswahl ein Jahresabschluss unterschiedliche Zahlen erzeugen.

Ein weiterer Schritt in die Zukunft wird sein, dass auch die Clients nicht mehr vom Unternehmen gewartet werden, sondern das ganze Betriebssystem mit benutzerangepassten Anwendungen über das Internet ins Unternehmen kommt. Das wird dann die sogenannte Applikations- oder Desktop-Virtualisierung sein. Deren Vor- und Nachteile werden dann bei entsprechender Marktrelevanz diskutiert, sicher ist, es wird sie geben.