

Netzheimer rät Praxistipps zum Einsatz von Web-Anwendungen



Web-Anwendungen – super Erfindung

Wer von Web-Anwendungen spricht, ist fast schon altmodisch. Heutzutage heißt es „Cloud-Anwendung“. „Cloud“ wird dabei als Synonym zum „Web“ verwendet – das ist zwar nicht ganz richtig, hilft aber, die Sache einzuordnen. Ich bleibe bei den Web-Anwendungen.

Web-Anwendungen haben Vorteile, vor allem, wenn die Software nicht auf dem eigenen Server, sondern auf dem eines Internet-Providers läuft. Denn funktioniert der Provider richtig gut, dann kann sich der Nutzer voll und ganz auf seine Rolle als Anwender zurückziehen und spart sich alles Kopfzerbrechen um Software-Updates, Sicherheitspatches oder technische Standards.

Halt, stimmt nicht ganz. Denn auch die Nutzer von Online-Anwendungen sollten sich an bestimmte Rahmen- und Sicherheitsbedingungen halten. Meine Praxistipps helfen Ihnen dabei, beim Betrieb Ihrer Web-Anwendungen die richtigen Maßnahmen zu ergreifen. Wenn Sie sich trotzdem nicht sicher sind, fragen Sie einfach den Internet-Dienstleister Ihres Vertrauens.

Ihr Felix Netzheimer



Online- oder Web-Anwendungen (auch Applikationen genannt) sind Computer-Programme, die auf einem Webserver laufen und vom Anwender über einen Browser bedient werden, z.B. Contentmanagementsysteme (Typo3, Joomla), Webshopsysteme (Magento, xtCommerce, osCommerce), Newslettersysteme (SuperMailer, Mailjet), E-Mail-Lösungen ...

Diese Anwendungen haben eine Reihe von Vorteilen, die deutlich zu ihrer Verbreitung beigetragen haben: Die Wartung und das Update muss nur noch an einer Stelle, nämlich auf dem Server im Internet, erledigt werden und nicht mühsam auf einzelnen Rechnern. Im Idealfall überträgt man diese Aufgaben an seinen Internetprovider, der die Anwendungen auf einem Server in seinem Rechenzentrum betreibt. Damit können Sie sich komplett auf die Nutzung konzentrieren.

Web-Anwendungen erfordern jedoch erhöhtes Sicherheitsbewusstsein: Da die eingesetzte Software nicht mehr im ab-

geschlossenen Firmennetz, sondern über das Internet genutzt wird, sind sorgfältige Sicherheitsvorkehrungen nötig. Das beginnt beim Sicherheitsbewusstsein der Mitarbeiter – Stichwort Passwortvergabe – und endet beim Einsatz der richtigen Firewall.

Prüfen Sie also genau, ob Ihr Unternehmen und Ihre Mitarbeiter für den Einsatz von Online-Anwendungen bereit sind. Am besten besprechen Sie mit Ihrem Provider Ihre Erwartungen und Vorstellungen, denn er übernimmt die Schlüsselrolle für einen sicheren und zuverlässigen Betrieb der Software im Web.



Praxistipps zum Einsatz von Web-Anwendungen

1. Checken Sie, welche Browser unterstützt werden

Web-Anwendungen sollten im Idealfall mit allen Internetbrowsern richtig funktionieren, was nicht selbstverständlich ist. Es gibt zwar Standards (W3C), verschiedene Browser und/oder unterschiedliche Browserversionen interpretieren den Quellcode der Seite trotzdem manchmal unterschiedlich. Ihre Anwendung sollte auf jeden Fall problemlos auf den wichtigsten laufen: Internet Explorer, Firefox, Safari oder Opera.

2. Setzen Sie auf das Minimalprinzip

So hübsch und praktisch Web-Anwendungen sind – hier gilt: je weniger, desto besser. Denn je mehr Anwendungen installiert sind, desto mehr Anwendungen sind auch angreifbar. Wenn Sie zum Beispiel keinen ftp-Service brauchen, sollte auch kein ftp-Server laufen.

3. Sensibilisieren Sie Ihre Mitarbeiter

Eine sehr effektive Methode, mit der Hacker Passwörter ausspionieren, ist weniger technischer als sozialer Natur. Die Nutzung von simplen Passwörtern aus dem sozialen Umfeld des Users gehört ebenso dazu wie simple Anfragen oder freiwillige Angaben etwa von Auszubildenden. Sie sind es als „Digital Natives“ gewohnt, sehr freizügig mit der Angabe von Daten und Informationen etwa in Facebook umzugehen. Sorgen Sie bei Ihren Mitarbeitern also für ein ausgeprägtes Sicherheitsbewusstsein.

4. Verwenden Sie sichere Passwörter

Sichere Passwörter sind ein ganz einfaches Mittel, Online-Anwendungen sicher zu machen. Leider wird es aus Bequemlichkeit zu selten genutzt. Ein Tool zum Prüfen, ob Sie ein sicheres Passwort verwenden, stellt beispielsweise der Kanton Zürich zur Verfügung. (<https://passwortcheck.datenschutz.ch/check.php?lang=de>).

Und vergessen Sie nicht, auch Ihren Applikationsanbieter unter die Lupe zu nehmen. Prüfen Sie, wie er Ihre Passwörter verwaltet. Denn das sicherste Passwort nutzt nichts, wenn es für andere einsehbar gespeichert wird.

5. Immer auf dem aktuellsten Stand halten

Für die meisten Web-Anwendungen werden in regelmäßigen Abständen Sicherheitsupdates veröffentlicht. Diese sollten grundsätzlich immer installiert werden, um neu entdeckte Sicherheitslücken zu schließen. Wenn Sie sich nicht fortwährend über die neuesten Updates Ihrer Web-Anwendungen informieren wollen und können, ist

es sinnvoll, diesen Prozess an Ihren Hoster/Provider auszulagern. Informieren Sie sich vor der Entscheidung für einen Hoster, ob er diesen Service bietet.

6. Nur die richtige Firewall schützt richtig

Klassische Firewalls, die sich auf die Überwachung von Ports konzentrieren, können Web-Anwendungen nicht hinreichend schützen. „Next Generation Firewalls“ wie etwa die von Palo Alto Networks (www.paloaltonetworks.com) hingegen oder „Web Application Firewalls“ analysieren und kontrollieren die Protokolle der Programme und schauen in die Datenströme. So erkennen sie gefährliche Daten und können sie blockieren.

7. Programmierfehler sind Einfallstor für Malware

Durch eine unsichere oder fehlerhafte Programmierung entstehen die meisten Sicherheitslöcher auf Ihrem Webserver. Achten Sie deshalb bei der Einrichtung und der Verwendung Ihrer Anwendung auf eine saubere Programmierung. Die enge Abstimmung mit Ihrem System-Administrator oder Ihren jeweiligen Dienstleistern ist ein sehr wichtiger Punkt. Einen anschaulichen Überblick über mögliche Programmierschwachstellen finden Sie:

- im Artikel „Wenn die Webanwendung zur Sicherheitslücke im Firmennetz wird“ auf dem Sicherheitsportal www.searchsecurity.de. (<http://www.searchsecurity.de/themenbereiche/applikationssicherheit/webapplication-security/articles/170064/>)
- oder bei Wikipedia unter dem Schlagwort „IT-Sicherheit“
- oder auf der Website des Projektes „Open Web Application Security Projekt“ (<http://www.owasp.org/index.php/Germany>)

8. Sensible Daten verschlüsselt übertragen

Auch derzeit werden immer noch viel zu viele Daten unverschlüsselt versandt. Dabei ist Verschlüsselung nicht nur für die unternehmenskritische Übertragung der Daten essenziell, sondern auch für den Betrieb eines Webshops ein absolutes Muss, um Vertrauen bei den Online-Kunden zu schaffen.

9. Wählen Sie Ihren Dienstleister sorgfältig aus

Da das Gros der Web-Applikationen in externen Rechenzentren bei Internet Providern betrieben und gehostet wird, ist es wichtig, dem Dienstleister genau auf den Zahn zu fühlen, ob er Ihren Sicherheitsansprüchen gerecht wird. Ansonsten sind die Lücken nicht in Ihrem Unternehmen, aber vielleicht bei Ihrem Provider. Eine Hilfe bei der Auswahl des geeigneten Dienstleisters sind vor allem Zertifizierungen und Referenzen, die Aufschluss über seine Qualifikationen geben.