Sicherheit im Web 2.0 für Groß und Klein

Die Anforderungen der Sicherheit an die IT-Systeme haben sich durch das neue Internet und die dort angebotene Dienste deutlich geändert. Welche Gefahren sich durch die neuen Anwendungen ergeben und welche Schutzmechanismen zur Verfügung stehen, zeigt dieser Artikel auf – interessant nicht nur für IT-Experten, sondern für jeden Internet-Nutzer.

Um zu verstehen wie vielfältig heute die Anforderungen an die Sicherheitssysteme sind, muss man den Wandel der Dienste im Internet sehen. Es ist noch gar nicht so lange her, da bestand das Internet aus passiven Inhalten wie Texten, Grafiken und Bildern. Der Browser war eine einfache Anwendung, der ausschließlich in der Lage war, diese statischen Inhalte anzuzeigen.

Mit der Zeit wurden die Inhalte immer „aktiver“ mit Animationen, Ton und Videos. Damit die Browser dieser Inhalte wiedergeben konnten, wurden sie mit Zusatzmodulen ergänzt. Dann kam die Zeit der Java-Anwendungen mit noch mehr Dynamik.

Heute stehen eine Vielzahl an Diensten im Internet zur Verfügung – dokumentiert unter dem Begriff „Web 2.0“. Dieser steht so zu sagen für die nächste Generation der Internet-Inhalte: Hier ersetzen Online-Anwendungen die lokalen Programme auf dem Computer und laufen für den Nutzer wie ein herkömmliches Programm, aber im Browser.

Dieser Generationswechsel stellt natürlich andere Anforderungen an die Systeme und an die IT-Sicherheit. Da sich das Web 2.0 mit all seinen Möglichkeiten immer weiter ausbreiten und entwickeln wird, ist ein Verzicht darauf natürlich der falsche Ansatz.

Anwendungen laufen im Web

Das Web 2.0 hat einen Prozess in Bewegung gesetzt, der mittelfristig eine grundlegende Veränderung bei den Anwendungen mit sich bringen wird. Dieser Trend ist schon sichtbar, beispielsweise bei den Webmail-Diensten: Oft stehen die von den Webdiensten angebotenen Funktionen denen eines eMail-Clients auf dem lokalen Rechner in nichts nach, aber sie laufen nicht auf dem Rechner, sondern im Internet und öffnen damit Sicherheitslücken.

Zweifelsfrei bietet das Web 2.0 auch Vorteile: Der Benutzer benötigt nur noch einen Browser. Die Installation einer lokalen Anwendung ist überflüssig. Diesem Trend folgen immer mehr Applikationen. Google & Co. haben es vorgemacht: Sie stellen Dienste wie Mail, Kalender, Textverarbeitung und Tabellenkalkulation online zur Verfügung. Selbst Bildbearbeitung ist schon im Web verfügbar. Wo die Daten dann gespeichert werden und wie sicher sie dort sind, steht natürlich auf einem anderen Blatt.

Auch Microsoft hat dies erkannt und mit den Web-Anwendungen eine Konkurrenz bekommen, die dem Marktführer langfristig weh tun kann. Daher baut das kommende Windows 7 als Nachfolger von Vista auch auf Anwendungen im Web.

Die neue Sicherheit

Bei diesen neuen Applikationen greifen die herkömmlichen Sicherheitsmechanismen nicht mehr. Die Zeiten sind längst vorbei, als noch eine einfache Firewall und ein Virenscanner ausreichenden Schutz boten. Durch die neuen Anwendungen, die sich deutlich von den „lokalen“ unterscheiden, müssen die Schutzmechanismen angepasst werden.

Schutz für jede „Größe“

Mit geeigneten Maßnahmen können Unternehmen eine Sicherheit darstellen. Dabei spielt es keine Rolle, ob es sich um das Büro eines Selbstständigen oder einen kleinen Familienbetrieb handelt oder ob es um die Absicherung großer Unternehmen mit Niederlassungen geht. Auf dem IT-Security Markt gibt es derzeit aber nur wenige Hersteller, die diese unterschiedlichen Zielgruppen abdecken. Aber es gibt sie, und hier liegt der Vorteil für die „Kleinen“: Sie profitieren vom Wissen der Hersteller, die Sicherheitssysteme für große Unternehmen realisieren. Das Knowhow steht damit auch kleinen Büros zur Verfügung.

Der erste Schritt zur sicheren Nutzung der neuen Web-Dienste ist für jede Unternehmensgröße gleich. Die Anforderungen an die Kommunikation müssen festgelegt werden. Dabei kann ein uneingeschränkter Zugriff der Mitarbeiter auf das Internet nicht im Sinne des Unternehmens sein. Hier gilt es, die Web-Verbindungen auf das benötigte Minimum zu beschränken und wenn möglich zu zentralisieren, z. B. über einen Proxy-Dienst. Dies erleichtert die Überwachung der Daten und Verbindungen. Um hier Missverständnissen vorzubeugen: Es geht hier nicht um die Überwachung von Mitarbeitern, sondern um die Kontrolle der Verbindungen auf sogenannten Schadcode hin. Und das ist im Web 2.0 wichtiger denn je.

Angriff von allen Seiten

Die Angriffsszenarien haben sich geändert. Schadcode wird längst nicht mehr nur von Webseiten (im Volksmund „Schmuddelseiten“ genannt) verteilt, die nicht zum geschäftlichen Umfeld gehören. Da sich geschäftliche Webseiten immer mehr Content Management Systemen bedienen, steigt auch das Risiko, den Betreibern heimlich Schadcode „unterzuschieben“, wenn sie ent sprechende Seiten besuchen.

Einfallstor Emails

Das kann auch durch das Öffnen einer eMail passieren. Immer mehr Mails enthalten nicht mehr alle Inhalte. Sie laden diese aus dem Internet nach, z. B. Bilder oder Animationen. Da aber das verbreitete Outlook den Internet Explorer zur Anzeige der Mails verwendet, werden so automatisch diese Inhalte in einem Browser ausgeführt, als würde die Webseite direkt besucht werden.

Die Grenzen zwischen den Applikationen verschwimmen, wie auch die Quelle der Inhalte. Für den Anwender ist kaum mehr zu unterscheiden, aus welcher Quelle die Daten stammen – ob diese lokal sind oder aus dem Internet kommen. Aus diesem Grund braucht es geeignete Schutzmechanismen, die sowohl die „klassischen“ Gefahren abwehren wie auch den neuen Gefahren entschieden entgegentreten können. Dabei ist es möglich, zumindest auf das Sicherheitsniveau wie zu Zeiten des Web 1.0 zu kommen.

Weil die Anforderung für die benötigte Kommunikation von Unternehmen zu Unternehmen sehr unterschiedlich sind, gibt es keine Pauschallösungen. Aber mit geeigneten Konzepten und Systeme sowie dem Verständnis dafür, dass Sicherheit keine statische Sache ist, sondern ein stetiger Prozess, können sich Firmen wirkungsvoll schützen und trotzdem alle Vorteile des Web 2.0 nutzen.

Die geänderten Rahmenbedingungen und Gefahrenlagen bedürfen mehr denn je einer individuellen Beratung. Standardlösungen helfen in der Regel nicht umfassend.

Inhalte und Wege checken

Security Systeme, die dem Stand der Technik entsprechen, analysieren Inhalt und Aufbau von Mails bis ins kleinste Detail und können daher versteckten Schadcode erkennen. Dabei wird auch der „Datenweg“ berücksichtigt, den das Mail zum Anwender genommen hat.

Webseiten werden nach Sicherheitskategorien gelistet und sperren gefährliche Seiten sofort. Selbst Suchmaschinenlisten werden so durchforstet, dass entsprechende Seiten erst gar nicht bis zum Anwender durchkommen. Das ist Sicherheit auch im Web 2.0.

salutec
www.salutec.de

Zum Autor:
Michael Schmidt arbeitet seit über 10 Jahren im IT-Security-Umfeld. Er ist TÜV-zertifizierter Datenschutzbeauftragter sowie Geschäftsführer der salutec GmbH (Haiger) für den Bereich Security.