Softwaresicherheit – ein realistisches Ziel?

Um gleich die Brücke vom Schwerpunkt dieses Heftes zu den kulturellen (und ideellen) Werten des Datenschutzrechts zu schlagen: Neben das seit dem Volkszählungsurteil des Bundesverfassungsgerichts (BfG) von 1973 verankerte Recht auf informationelle Selbstbestimmung ist über das Urteil des BfG zu Vorschriften des Verfassungsschutzgesetzes Nordrhein-Westfalen zur Online-Durchsuchung und zur Aufklärung des Internet vom 27.02.2008 ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme getreten.

Das klingt sehr plausibel, ruft aber gleichzeitig zu einer Bewertung der realen Situation bei allgemein verfügbaren Informationstechnologien auf. Die tägliche Nachrichtenlage und die inzwischen weit verbreiteten Warnzeichen für den Sicherheitsstatus, die durchgängig erhöhtes oder hohes Risiko signalisieren weisen darauf hin: Vertraulichkeit und Integrität der IT-Umgebung eines Nutzers werden laufend bedroht und häufig verletzt, und zwar nicht durch das BKA oder den Verfassungsschutz, sondern durch Schadsoftware, die den Angreifern Profit verschafft. Hacker suchen längst professionell organisiert nach Schwachstellen in Betriebssystem- und weit verbreiteter Anwendungssoftware, finden laufend neue Sicherheitslücken und nutzen diese aus. Die übliche Gegenreaktion der Softwareanbieter besteht darin, möglichst zeitnah Sicherheitsupdates zum Schließen der entdeckten Software-Schwachstellen anzubieten. Nur dann, wenn die Software auf den Rechnern der Anwender mit dem Update gepatcht worden ist, hat der Angreifer verloren. Um ein möglichst hohe Updatereichweite zu unterstützen, werden den Nutzern häufig automatisierte Updateverfahren angeboten, durch die natürlich die informationstechnische Integrität ihrer Systeme verletzt wird.

Dieser reaktive Ansatz ist langfristig nicht zielführend, da Anwender immer zeitweise Angriffen ausgesetzt sind, bis ein Patch geliefert werden kann. Sichere Software kann lediglich mit einem proaktiven Ansatz, der im Softwareentwicklungsprozess verankert ist, gewährleistet werden. Das Ausliefern von Patches sollte idealerweise nur wenige Fälle betreffen, die durch das Netz der Qualitätssicherungsmaßnahmen geschlüpft sind.

Noch weitaus komplexer werden die Zusammenhänge, wenn geschäftskritische IT-Anwendungen betrachtet werden. Hier sind Software-Schwachstellen Ursache für nicht kalkulierbare Risiken und damit auch für die Verletzung von gesetzlichen Vorschriften (Compliance) mit ökonomischen oder rechtlichen Folgen. Entsprechend hoch sind die technischen und organisatorischen Aufwände, um die IT-Systeme angemessen gegen Angriffe zu sichern.

Die Softwareindustrie setzt nun verstärkt auf proaktive Maßnahmen. Das Beispiel SAFE-Code wird im Gateway dieses Heftes beschrieben.

Zu diesem Heft:

Unsere Zeitschrift versammelt in diesem Heft Beiträge international anerkannter Experten, die auf ihrem Gebiet eine weitere Verbesserung der Softwarequalität vorantreiben. Damit soll dieses deutsch-englische Heft auf der CeBIT 2010 und auf der RSA Conference 2010 über den traditionellen Leserkreis hinaus wirken.

Der Beitrag von *Steve Lipner* stellt dar, wie die Prinzipien der sichereren Softwareentwicklung bei Anwendungen im Cloud Computing einzusetzen sind. *Kai Jendrian* beschreibt die Standardisierung der Sicherheitsüberprüfung von Web Anwendungen nach dem Modell der OWASP. *Maty Siman* stellt eine Plattform zur Code Analyse hinsichtlich Sicherheitslücken von Anwendungen vor. Dies liefert einen wesentlichen Beitrag, um Sicherheit proaktiver zu gestalten. Darauf aufbauend liefert der Beitrag von *Chess* und *West* einen Ansatz die Ergebnisse solcher Testautomaten nach Risiko für den Anwender zu priorisieren. Abschließend gehen *Wysopal*, *Eng* und *Shields* auf die Detektion von vorsätzlich in den Code eingefügter „Hintertüren“ ein. Ein politisch derzeit sehr spannendes Thema, denn Software könnte auch bewusst als Waffe benutzt werden, um dem Anwender zu schaden.

Dies alles liefert uns im Jahre 2010 noch keine Garantie der „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ aber das Ziel wird realistischer.

Gunter Bitz, Helmut Reimer