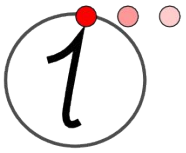
D.A.CH. Security 2005

Ein subjektiver Teilnehmerbericht

VON GERD STOLPMANN, GERD@GERD-STOLPMANN.DE

VOM 26.04.2005, ÜBERARBEITET 12.06.2005

Vom 15. bis 16. März fand in Darmstadt die Konferenz D.A.CH. Security 2005 statt. Gerd Stolpmann berichtet von seinen Eindrücken.



Informatikbüro
Dipl.-Inform. Gerd Stolpmann

Viktoriastr. 45 • 64293 Darmstadt
http://www.gerd-stolpmann.de

D.A.CH Security 2005 – Ein subjektiver Teilnehmerbericht

Eigentlich bin ich über diese Konferenz eher zufällig gestoßen, ein Artikel im Heise-Newsticker machte mich auf diese Veranstaltung aufmerksam, die auch noch zufällig keine 500 Meter von meinem Büro entfernt stattfand. Der Untertitel „Bestandsaufnahme – Konzepte – Anwendungen – Perspektiven" macht deutlich, dass die Konferenz einen Überblickscharakter hat. Die Veranstalter wollen, nach eigener Aussage, Anbieter und Anwender zusammen bringen. Ein Blick auf die Teilnehmerliste zeigte jedoch, dass die Anbieter klar in der Überzahl waren. Es gab wenige Anwender aus den Großkonzernen, und fast gar keine aus dem Mittelstand. Möglicherweise lag das an der parallel stattfindenden Cebit-Messe, aber dennoch bleiben leise Zweifel, ob das Thema IT-Sicherheit bei den Anwendern angekommen ist.

Die Anwender wären jedenfalls gut beraten, kritisch mit den Anbietern ins Gericht zu gehen. Naturgemäß wollen die Hersteller vor allem ihre Produkte verkaufen, und da IT-Sicherheit ein unübersichtliches Terrain ist, scheint die Meinung verbreitet zu sein, man könne den Anwendern alles verkaufen, was irgendeinen Zugewinn an Sicherheit verspricht. Der Vortrag von Detken und Götsche[i] machte jedoch deutlich, dass nicht alles Gold ist, was glänzt. Intrusion Detection Systeme (IDS), schon lange ein gängiger Begriff, taugen offenbar nicht und sind ihr Geld nicht wert. Das liegt daran, dass diese Systeme, ähnlich wie Virenscanner, mit Signaturen arbeiten, aber die tatsächlich stattfindenden Angriffe sich gar nicht in die Muster einordnen lassen, die den Signaturen zu Grunde liegen. Die Vortragenden gaben den IDS noch eine zweite Chance, wenn die Hersteller sie lernfähig machen würden – im Augenblick unterstützt dies jedoch kein Produkt. Interessant war auch die Aussage der Vortragenden, dass sich kommerzielle und Open-Source-Lösungen in der Qualität nicht wesentlich unterscheiden (beide sind gleich schlecht).

Letztlich gilt immer noch, dass es besser ist, die IT-Landschaft eines Unternehmens von vorne herein mit sicheren Komponenten aufzubauen, als die Sicherheit hinterher mit Zusatzprodukten „hineinzupatchen", die oftmals einen fragwürdigen Nutzen haben. Meiner Meinung nach gilt dies grundsätzlich auf für etablierte Zusatzprodukte wie etwa Virenscanner – einige Unternehmen begreifen inzwischen die Lehre und stellen Arbeitsplätze auf Linux um.

Ein Großteil der Konferenz befasste sich mit Sicherheits-Infrastrukturen, wie z.B. PKI oder Single Sign On. Mich haben diese Themen nicht so stark interessiert, weil sie häufig unter Management-Gesichtspunkten diskutiert worden sind. Es stand häufig die Frage (ungestellt) im Raum, wie man ein Mehr an Sicherheit bei Reduktion der Kosten erreichen kann. Infrastrukturen sind nämlich teuer und stehen unter einem Rechtfertigungsdruck, es stellt sich dann schnell die Frage, welche Kompromisse man eingehen kann, um akzeptable Sicherheit zu geringeren Kosten zu

bekommen. Ein Beispiel für einen fragwürdigen PKI-Ansatz werde ich gleich skizzieren.

Meiner Meinung nach auf der Konferenz zu kurz gekommen sind Ansätze, wie Entwickler in die Lage versetzt werden können, sichere Software herzustellen. Siehe oben: Besser, ein Unternehmen setzt von vorne herein auf sichere Komponenten. Aber wie bekommt man diese? Der Vortrag von Stormer und Knorr[ii] zeigte exemplarisch an der Web-Shop-Lösung eSarine, wie Sicherheit sowohl konzeptuell als auch in der Kodierungs-Praxis Einzug halten kann. Im Grunde wurde nichts neues vorgestellt: Web-Anwendungen haben typische potenzielle Sicherheitslöcher, von denen einige durch konzeptuelle Maßnahmen in den Griff zu bekommen sind und einige schlicht durch Programmierdisziplin in Schach gehalten werden können. Trotz der fehlenden Novitäten war dies ein notwendiger Vortrag, da er überdeutlich zeigte, wie leicht es Angreifer haben, die auf Web-Anwendungen zielen, und wie schwer es Hersteller haben, die Abwehrmaßnahmen zu organisieren. Angreifer bekommen nämlich einen Teil der Informationen, die sie benötigen, frei Haus geliefert, wenn sie sich den HTML-Quelltext anschauen. Die Hersteller haben dagegen das Problem, einheitliche Qualitätsstandards im gesamten Quellcode des Produkts zu etablieren.

Es stellt sich die Frage, ob letzteres nicht auch ein Versagen der klassischen Entwurfsmethoden für Programme ist. Kühnhauser und Welsche[iii] zeigten in ihrem Beitrag, dass es Auswege gibt. Workflow-Systeme kann man nämlich sehr gut mit formalen Methoden angehen und damit Sicherheitseigenschaften nicht nur auf der konzeptuellen Ebene nachweisen, sondern durch das Hineinziehen des Formalismus in die Implementierung auch direkt letztere profitieren lassen. Die Autoren modellierten ein Workflow-System mit Hilfe von mehrschichtigen Petri-Netzen. Wenn man diese Netze direkt implementiert und nicht nur als Meta-Beschreibung ansieht, etabliert man ein recht starkes Sicherheitsprinzip direkt im Code. Meiner Meinung ist das der Königsweg, wie Anwendungen sicher gemacht werden können. Natürlich, und das ist eben betrüblich, braucht man in der Praxis dann auch gute Informatiker, die etwas von formalen Modellen verstehen. (Aufruf an alle Studenten: Beschäftigt euch wieder mehr mit theoretischer Informatik, und lasst euch nicht so sehr von der Hektik der Praxis einschüchtern!)

[In der ersten Fassung gab es hier noch einen Abschnitt über ein Projekt der kassenzahnärztlichen Vereinigung Baden-Württemberg. Da dieser einen, auch aus Sicht des Autors, falschen Eindruck erweckt hat, wurde er aus der Veröffentlichung genommen. Ggf. folgt eine überarbeitete Fassung. - G.S.]

D.A.CH Security, veranstaltet vom Darmstädter Zentrum für IT-Sicherheit

- Tagungsband: „D.A.CH Security 2005 – Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven“, hrsg. von Patrick Horster, syssec, ISBN 3-00-015548-1

i „Intrusion Detection und Response – Anforderungen, Analysemethoden und Systemunterschiede“, von Kai-Oliver Detken und Dirk Göttsche. Im Tagungsband.
ii „Sicheres Web Shopping – Das eSarine Projekt“, von Henrik Stormer und Konstantin Knorr. Im Tagungsband.
iii „Sicherheitsmodelle für computergestützte Teamarbeit“, von Winfried E. Kühnhäuser und Gabriel Welsche. Im Tagungsband.