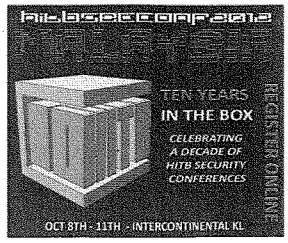

Hack in the Box 2012: Einblick in fremde Welten

Kulturclash

Bernd Wernerus

Ob Vorträge von Hacker-Legenden über die „guten alten Zeiten" oder Beiträge über die für Europäer merkwürdigen asiatischen Gepflogenheiten – die Jubiläumsveranstaltung der „Hack in the Box" bot erhellende Einblicke in Welten aller Art.

Die zehnte Security-Konferenz „Hack In the Box" in Kuala Lumpur (10./11.Oktober 2012) glänzte mit einem großen Staraufgebot. Zu Beginn der Veranstaltung erläuterten die für ihre Kreditkarten-Hacks bekannten Italiener Andrea Barisani und Daniele Bianco in ihrem Vortrag „Practical Exploitation of Embedded Systems", wie man die Debugging-Schnittstellen der Hardware (zum Beispiel JTAG oder serielle Schnittstelle) findet oder über Manipulation des Kernels Debug-Ausgaben erzeugt. Mit den daraus stammenden Informationen kann ein Angreifer das Zielsystem verstehen und angreifen.

Als ein Urgestein der IT-Security Szene hielt John „Captain Crunch" Draper einen „historischen" Vortrag über die Geschichte der Personal-Computer- und Phreaking-Szene. Teilweise war der Vortrag mit witzigen Anekdoten gespickt, unter anderem über Drapers gemeinsame Zeit mit Steve Jobs und Steve Wozniak zu Zeiten des Homebrew Computer Club. Leider gingen die Anekdoten häufig in der wirren und manchmal etwas verbitterten Art von Captain Crunch unter. Nichtsdestotrotz kann man auf seine aktuellen Projekte gespannt sein – ein Buch sowie ein Film stehen auf der Agenda.

Der Abschluss des ersten Tages war mit dem Vortrag „I Honorably Assure You: It is Secure – Hacking in the Far East" von dem in Japan lebenden Deutschen Paul Sebastian Ziegler wieder amüsanter: Mit Rückblick auf seine Erfahrungen als Pentester in Japan und Südkorea verdeutlichte er den Zuschauern, welche Sicherheitsimplikationen kulturelle Unterschiede haben können. Darunter fällt etwa die Tatsache, dass in Japan alle Angestellten einen großen Teil ihres Gehalts in Form von Boni erhalten. Diese werden typischerweise nicht nach Leistung, sondern nach Überstunden berechnet und nur dann gestrichen, wenn der Angestellte Fehler macht. Nichts zu tun schützt folglich vor Fehlern. Das führt dazu, dass man sicherheitsrelevante Änderungen nur schwer umsetzen kann, weil niemand bereit ist, die Verantwortung für sie zu übernehmen.

Im Vortrag „How to Get Along with Vendors Without Really Trying" gab Katie Moussouris einen Ausblick auf einen kommenden ISO-Standard, der den Umgang von Produktherstellern mit Schwachstellenmeldungen definiert. Reagieren Hersteller auf die Entdeckung von Schwachstellen in ihren Produkten bislang noch allzu oft mit Ignoranz oder gar Sanktionen gegen den Entdecker, so fördert der Standard die Zusammenarbeit mit dem Sicherheitsforscher, das Beheben der Schwachstelle und die Suche nach den Ursachen.

HTML5: Sicher und doch problematisch

Shreeraj Shah erläuterte eindrucksvoll, welche Probleme HTML5 mit sich bringt – sowohl in Form von neuen Angriffen als auch durch alte Angriffe, die durch HTML5 noch erleichtert werden. Besonders bemerkenswert sind hier unter anderem die Funktionen zur clientseitigen Speicherung von Daten in einem Dateisystem oder einer Datenbank im Browser. Überdies lassen die Erweiterungen in HTML5 in gewissen Konstellationen Cross-site-Request-Forgery-Angriffe zu, die die Cross Domain Boundary des Browsers umgehen. Dies ermöglicht es einem Angreifer, nicht nur einzelne Requests im Kontext des Opfers zu generieren, sondern, mittels JavaScript, auch problemlos mehrere Requests in Folge. Unter Umständen kann er sogar auf die Antworten des Servers zugreifen und sie mithilfe von JavaScript auswerten. In dem Fall lassen sich Abläufe in Webanwendungen mit mehreren Schritten abbilden und somit angreifen.

Chris Evans von Google erläutert Schritt für Schritt wie der jüngste, direkt vor Ort demonstrierte Zero-Day für den hauseigenen Browser Chrome funktioniert. Der Chrome-Exploit verwendete eine Use-after-Free-Schwachstelle – also ein Fehler, der beispielsweise beim Zugriff auf ein schön gelöschtes Speicherobjekt auftritt – in der SVG-Engine des Browsers, um innerhalb der Sandbox eigenen Code zur Ausführung zu bringen. Chrome ist in Sicherheitskreisen jedoch bekannt dafür, dass der Ausbruch aus seiner Sandbox nicht trivial ist. Das Ungewöhnliche an dem Exploit ist daher, dass er eine Funktion zum Speichern von Dateien im Dateisystem ausnutzt. Diese war aus historischen Gründen noch in der Sandbox enthalten und verlangte vor dem Speichern keine Bestätigung durch den Benutzer.

Den Abschluss der Konferenz bildete eine Auktion zugunsten einer malaysischen Krebsklinik. Die Moderatorin überredete den in Sicherheitskreisen bekannten finnischen Chief Research Officer von F-Secure Mikko Hypponen dazu, einen Großteil seiner langen Haare für den guten Zweck zu opfern. Die gesamte Konferenz wurde auf Video aufgezeichnet. Somit sollten die Vorträge über kurz oder lang im Internet zu finden sein – einschließlich des „Pferdeschwanzopfers" von Hypponen. (ur)

Kurz notiert

Bilderklau 2.0: Trend Micro hat eine Drive-by-Schadsoftware entdeckt, die auf ältere Windows-Betriebssysteme zielt und Bilddateien sowie Speicherabbilder stiehlt. Die Experten vermuten, dass die Informationen gezielten Angriffen (Social Engineering) auf Unternehmen dienen sollen.

Cybermafia: Ebenfalls von Trend Micro stammt eine ausführliche Analyse des osteuropäischen Cybercrime-Marktes (s. „Alle Links"). Beschrieben sind sämtliche Services wie Hacking, Social Engineering, Spamming, Rootkits und Verschlüsselung et cetera sowie deren Preise. Einen Denial-of-Service-Angriff auf ein Wunschziel erhält man schon für 30 Dollar pro Tag.

Schwachstellenmanagement: Secunia stellt Version 4.0 seines Vulnerability Intelligence Manager (VIM) vor. Neben der verbesserten Benutzeroberfläche haben die Entwickler an der Integration in das Patchmanagement-Werkzeug CSI, dem Asset-Abgleich sowie dem Datenexport gearbeitet. Außerdem haben sie ein Aktivitätenlogging integriert.

Serverüberwachung: SSC stellt eine Freeware-Version (s. „Alle Links") seiner Monitoring-Software „Server Inspector" zur Verfügung. Sie überwacht Betriebssysteme, Netzwerke und Datenbanken et cetera und warnt per Mail oder SMS. Der Funktionsumfang ist gegenüber der Vollversion eingeschränkt, mit ihr lässt sich nur ein Server überwachen.