IT-Defense 2010, 3. bis 5. Februar, Brühl

Gefühlte Sicherheit

von Daniel Richey

IT-Sicherheit geht weit über Antivirus, Firewalls und Intrusion Detection hinaus. Wie weit, das zeigte die IT-Defense 2010 in Brühl. Eine breite Palette an On- und Offline-Sicherheitsthemen gab den rund 200 Teilnehmern Denkanstöße und rüttelte so manchen IT-Administrator wach.

Gespannt lauschten die rund 200 Teilnehmer der IT-Defense Anfang Februar Moxie Marlinspike, als er grundlegende Schwachstellen in SSL erläuterte. Diesmal ging es nicht um Angriffe auf die Algorithmen oder die zugehörige Software. Marlinspike vom Institute for Disruptive Studies verdeutlichte vielmehr, wie leicht sich Zertifikate von echten Zertifizierungsstellen – den sogenannten CAs – erschleichen lassen. Mit einem einfachen Trick bei der Beantragung der Zertifikate lassen sich Browser, Mailclient und Co. austricksen. So reicht es laut Marlinspike aus, in den Online-Antrag einen sogenannten Nullcharacter einzufügen, also etwa *www.bank.de\0.hackerdomain.com*. Die Zertifizierungsstelle erkennt den Antrag korrekterweise auf hackerdomain.com und stellt das Zertifikat entsprechend aus. Doch der Browser interpretiert den Nullcharacter anders und nimmt das Zertifikat für *www.bank.de* an. Opera hat als erster Hersteller hier versucht, den Fehler zu beheben – wenn auch nicht sonderlich erfolgreich. Doch sollen nach diversen Berichten inzwischen die Software-Hersteller diesen Fehler behoben haben.

Ein Bein im Knast

Auf ebenfalls sehr großes Interesse stieß der Vortrag von Prof. Thomas Hoeren, Richter am Oberlandesgericht Düsseldorf. Er verdeutlichte, wie schnell ein IT-Verantwortlicher durch das Bundesdatenschutzgesetz persönlich zur Kasse gebeten werden kann – auch wenn er angestellt ist und auf Anweisung hin arbeitet. Welche abstrusen Urteile deutsche Gerichte dabei mitunter fällten, zeigte Hoeren an einigen Beispielen auf. Ein Mitarbeiter etwa klagte, weil der Administrator einen Spamfilter im Netzwerk einsetzte – und bekam vom OLG Karlsruhe Recht. So sei Spam in erster Linie Post und unterliege dem Briefgeheimnis. Nur bei einer gleichzeitigen Einwilligung von Empfänger und Absender dürfe das Spam gefiltert werden. Bei unerwünschten Werbemails kein leicht zu erfüllendes Kriterium. Dass diese Rechtsprechung nicht auf die leichte Schulter genommen werden darf, verdeutlicht das hierfür zuständige Strafrecht.

Auch Administratoren, die sich für ihre Unternehmenswebseite als Admin-C eintragen lassen, setzen sich besonderen Risiken aus. Denn ein Admin-C haftet laut Hoeren etwa bei Werberechts-, Urheberrechts-, Verbraucherschutzverstößen und ähnlichem mit dem Privatvermögen. Zudem entgeht der Admin-C nur dann der Denic-Verantwortung, wenn der Domaininhaber ihn daraus entlässt. Trägt sich ein Mitarbeiter als "Verantwortlicher im Sinne des Presserechts" (ViSdP) ein, haftet er sogar für alles, was auf dieser Website passiert. Dazu zählen auch Links – selbst wenn auf einen Haftungsausschluss hingewiesen wurde. Das so gerne zitierte Urteil des LG Hamburg vom 22. Mai 1998 hat es laut Hoerer dabei übrigens nie gegeben.

Neues in Snort

Da Administratoren natürlich im Rahmen ihrer Tätigkeit auch den Netzwerkverkehr überwachen müssen, stellte Martin Roesch als Vater des Traffic-Analyse-Systems Snort die neue Version 3.0 vor. So beinhaltet das Tool nun neben einer IPv6-Unterstützung auch Multiprotocol Label Switching und Generic Routing Encapsulation. Um die Datenanalyse dabei zu beschleunigen, soll Snort künftig auch über ein Multithread Execution Model verfügen und Datenpäkchen gleichzeitig durch mehrere Engines laufen lassen können. Besonders legte Roesch Wert darauf, in der neuen Version 3 auch die Code-Basis bereinigt zu haben. So sei das Tool quasi von Grund auf neu entwickelt worden und alter Code beseitigt. Snort 3 besteht dabei aus zwei wesentlichen Komponenten.

Dies ist einerseits die SSP (Snort Security Platform), auf der die Analyse läuft und die die Applikationen kontrolliert. Die Engines sind daneben die Applikationen in Snort. Diese laufen auf SSP. Damit lassen sich praktische Anwendungen ausführen, etwa jede Traffic-basierte Applikation oder etwa Vulnerability-Scanner. Bei der Network Map andererseits lassen sich die Regeln anhand der im Netzwerk genutzten Geräte gruppieren und zuordnen. So muss eine Detection Logic nicht einen Windows-Server vor Linux-Exploits schützen und Snort kann darauf basierend die Regeln effizienter nutzen. Ein manuelles Einpflegen der Daten ist damit nicht mehr nötig und ein Angreifer verliert seinen Informationsvorsprung über die anzugreifenden Systeme.

Weitere Themen auf der IT-Defense 2010 waren unter anderem die Sicherheit des GSM-Mobilfunksystems, das McColo-Botnetz sowie das Social Engineering und Ausspähen von Daten ohne technische Hilfsmittel. Damit bot die Veranstaltung einen Einblick in das Thema Sicherheit, das weit über die üblichen Ansätze mit Firewall, UTM und Co. hinausgeht.