AK Sicherheit, 05.05.2010, Protokoll

Thema der Sitzung: Webserver als Virenschleuder

13:00 Registrierung

13.30 Begrüßung

Dr. Kurt Brand (AK-Leiter Sicherheit und Geschäftsführer der Pallas GmbH) und Roland Broch (Business Development, eco) begrüßen die Teilnehmer. Herr Dr. Brand führt in das Thema ein. Schutz vor Malware im Web – das ist derzeit das wichtigste Thema im Bereich der Internet-Sicherheit. Immer stärker gehen Infektionen mit Schadprogrammen von Websiten aus, die Zahl der Infektionen per E-Mail dagegen sinkt. Der Arbeitskreis Sicherheit des eco stellt in dieser Sitzung die wichtigsten Entwicklungen vor und zeigt, wie Serverbetreiber, Webseitenbetreiber und Internetnutzer gemeinsam der Verbreitung von Schadsoftware Einhalt gebieten können.

Das Problem Malware: Trends und Perspektiven

Christian J. Dietrich, Leiter des Forschungsbereichs E-Mail-Sicherheit und Botnetze am Institut für Internet-Sicherheit der FH Gelsenkirchen, erklärte zunächst das wachsende Malware-Problem: Es gebe 35.000 und mehr verschiedene gezählte Malware-Muster pro Tag. Für Botnetze, also Netzwerke von Computern, die per Malware ohne Wissen des Nutzers zusammengeschaltet und ferngesteuert werden, gebe es sogar schon eigene „Baukästen“, die das Programmieren der Schadsoftware vereinfachen. Diese tragen zwar zur Vermehrung von Malware bei, gleichzeitig sind aber Schadprogramme, die aus solchen Toolkits stammen, leichter zu erkennen. Über die Hälfte aller Schadprogramme erzeuge Netzverkehr, trage also zur Weiterverbreitung von Botnetzen bei. Bei der Erkennung von Botnetzen sei es sinnvoll, verhaltensanalytische Methoden auf Netzwerkebene einzusetzen; damit könnten auch verschlüsselte Botnetze erkannt werden.

XSS in the wild: How web attackers abuse the trust in your company

Elmar Johnen, Security Manager bei Vodafone D2, demonstrierte anschließend in einer Live-Session, wie Nutzer ihren Computer über den Besuch infizierter Websites mit Schadprogrammen infizieren können. Beim sogenannten Cross Site Scripting wird auf unterschiedlichen Wegen, wie z.B. über Sicherheitslücken in Webanwendungen wie Foren, Blogs und Gästebüchern, Schadcode in eine ansonsten seriöse und vertrauenswürdige Seite eingebunden. Ein solches Schadprogramm kann beispielsweise Eingaben des Nutzers wie Zugangsdaten protokollieren oder Pop-ups erzwingen, die zur Eingabe von Passwörtern auffordern.

Infiziert! Wer haftet?

Über die rechtlichen Auswirkungen von infizierten Websevern informierten dann *Dr. Thorsten Lieb* und *Nadja Wüstemann* von avocade Rechtsanwälte in ihrem Vortrag. Bei der vertraglichen Haftung seien beispielsweise Ansprüche eines Webseitenbesuchers beim Online-Einkauf gegenüber dem Betreiber denkbar, wenn dieser die verkehrsübliche Sorgfaltspflicht oder vorvertragliche Nebenpflichten ("keine Viren verbreiten") verletze. Hier wie auch bei der deliktischen Haftung ohne vertragliche Beziehung (z.B. bei Computersabotage) müsse der Geschädigte aber zur Durchsetzung seiner Anspüche Schaden, Kausalität und Verschulden nachweisen. Haftungsansprüche aus der deliktische Haftung seien aber in der Praxis bisher aber kaum durchgesetzt worden und insgesamt sei die Nachweisführung für alle Haftungsarten schwierig, die Gerichte würden sich vollständig auf Sachverständige verlassen. Für Webseitenbetreiber sei es dennoch wichtig, ihre Hoster vertraglich zu verpflichten, technische Vorsorge zu treffen und zu dokumentieren.

Erfahrungen mit verschiedenen URL-Filtern

Eine Möglichkeit, sich gegen Schadsoftware aus dem Web zu schützen, ist der Einsatz von URL-Filtern. *Stephan Sachweh*, Technischer Leiter der Pallas GmbH, zeigte die unterschiedlichen Möglichkeiten verschiedener Web-Filter: Browser-Filter im Internet Explorer und im Firefox sowie Gateway-Filter von Commtouch, McAfee (WebWasher) und

SonicWALL. Gerade Unternehmen sollten darauf achten, dass die eingesetzte Lösung für größere Installationen geeignet ist und sich flexibel konfigurieren lasse. Für die Zukunft würde die Klassifikation von Deep Links, also Webseiten tief im Angebot einer Website, sowie die Real-Time-Raktion auf Infektionen immer wichtiger. Die Filter zeigten auch teilweise signifikante Unterschiede in den Erkennungsraten.

Systemische Abwehr von Blended Threats

Um die systemische Abwehr von Blended Threats ging es im Vortrag von *Oliver Dehning*, Geschäftsführer der antispameurope GmbH. Unter Blended Threat werde ein Angriff auf die IT-Sicherheit verstanden, der mehrere Methoden nutzt, um sein Ziel zu erreichen. Um solcher Attacken Herr zu werden, reichen singuläre Maßnahmen nicht aus; vielmehr müssten ganzheitliche, systemische Ansätze gewählt werden. Expertenbetriebene Schutzsysteme in verschiedenen Schutzebenen seien dabei effektiver und kostengünstiger als Einzelmaßnahmen, insbesondere wenn man Cloud-Technologien nutze. Die besten Effekte ließen sich erzielen, wenn Hersteller und Betreiber zusammenarbeiten.

Verschiedenes, Themen und Termine

Zum Abschluss der Veranstaltung diskutierte der Arbeitskreis auf Anregung von Arbeitskreisleiter Dr. Kurt Brand, Geschäftsführer der Pallas GmbH, wie Serverbetreiber, Websitenbetreiber und Nutzer ihre Systeme gegen Schadprogramme aus dem Web schützen und deren Ausbreitung eindämmen können.

Websitebetreiber sollten:

- Web-Applikationen sicher entwickeln und eine sichere Softwarearchitektur verwenden
- In ihrer Website eingesetzte Fremdprogramme regelmäßig updaten (patchen), um potenzielle Sicherheitslücken zu schließen.
- Eine Web Application Firewall vorschalten

Internetnutzer können den Schutz ihres Computers verbessern, indem sie

- den Virenschutz auf dem aktuellsten Stand halten
- einen URL-Filter zwischenschalten, der kritische Seiten blockiert – Basisfuktionen bieten bereits die modernen Browser
- regelmäßig Updates für das Betriebssystem, alle wichtigen Programme und den Browser durchführen.

Serverbetreiber, die ihre Server selbst administrieren, sollten

- das System härten
- eine Firewall vorschalten
- auf Schadsoftware prüfen

Professionelle Serverbetreiber, Internetdienstleister und Antivirenhersteller können bei der Bekämpfung von Schadsoftware noch enger zusammenarbeiten. So helfen beispielsweise Informationen über versuchte Angriffe den Antivirenherstellern, neue Schadprogramme schneller zu erkennen.

Die Vorträge der Veranstaltung finden sich unter http://www.eco.de/arbeitskreise/1675.htm.

Ende der Sitzung: 18:00

gezeichnet: Dr. Kurt Brand, Leiter Arbeitskreis Sicherheit