'Shellshock und Mayhem sind ein brandgefährliches Duo'

"Shellshock und Mayhem sind ein brandgefährliches Duo"

Neues Botnet nutzt Shellshock-Schwachstelle
Ein Kommentar von Lucas Zaichkowsky, Enterprise Defence Architect bei AccessData
Die amerikanische Regierung warnte jüngst vor einer neuen Sicherheitslücke in Linux- und Apple Mac-Systemen. Der sogenannte Bash Bug gilt als ernstzunehmende Bedrohung, die sogar Heartbleed in den Schatten stellen würde. Mittels der als "Shellshock" bezeichneten Schwachstelle können Internetkriminelle Rechner und Webserver mit Schadsoftware infizieren und Daten stehlen. Clevere Angreifer haben das Potenzial der Sicherheitslücke schnell erkannt. Noch cleverere Angreifer gehen schon einen Schritt weiter: Sie nutzen Mayhem, ein auf Shellshock basierendes Botnet.
Externe Server, die die Shellshock-Schwachstelle aufweisen, sind extrem anfällig für Mayhem. Das Botnet befähigt Angreifer in mehrerer Hinsicht, Unternehmen und Usern enormen Schaden zuzufügen, beispielsweise durch das Stehlen sensibler Informationen wie Passwörter, persönliche Daten von Nutzern und Kreditkartendaten. Zusätzlich können infizierte Server dazu verwendet werden, um interne Systeme zu scannen und um schnell weitere Hintertüren zu öffnen. Durch Shellshock und Mayhem im Zusammenspiel erhalten Angreifer Zugang zu anderen internen Bereichen. Zum Beispiel können sie Shellshock verwenden, um auf einen Web-Server zu gelangen, der nicht zwingend als sensibel einzustufen und dadurch weniger geschützt ist. Mit diesem Server jedoch würde somit eine erste Hürde umgangen. Im Anschluss dient er als Ausgangspunkt für die ursprüngliche Absicht des Hackers. So fungieren Shellshock und Mayhem als brandgefährliches Duo für Cyberkriminelle.
Ein Rucksack voll mit Hacking-Tools
Wir können davon ausgehen, dass noch weitere, bereits vorhandene Hacking-Tools, Trojaner und Bot-Netze wie Mayhem verwendet werden, um die Shellshock-Lücke zu nutzen. So können Hacker auf ein ganzes Füllhorn an Tools zurückgreifen, um fremde Systeme zu infiltrieren. Bildlich gleicht dies einem Einbrecher mit einem Rucksack voll mit Werkzeug, um verschlossene Fenster und Türen aufzubrechen.
Unternehmen weltweit sollten daher reagieren und ihre Systeme bis ins kleinste Detail überprüfen. Ein gutes Intrusion Detection System kann schon die Lösung sein. Wichtig ist es, Angriffe einerseits zu erkennen und andererseits auch zu dokumentieren. Tiefe Systemscans und das Installieren neuester Patches sind ebenfalls Pflicht.
Über AccessData:
Die AccessData Group ist Entwickler von Incident Resolution-Lösungen auf dem neuesten Stand der Technik. Sie ermöglichen detaillierte Echtzeit-Einblicke, Analysen und eine schnelle Reaktion bzw. Aufklärung von Datenzwischenfällen. Dazu zählen u.a. Cyberbedrohungen, Insider Threats, mobile bzw. BYOD-Risiken, GRC (Governance Risk
 Compliance) sowie E-Discovery-Vorfälle, die sich aufgrund des immensen Datenvolumens (Big Data) häufen. Mehr als 130.000 User, die weltweit im Gesetzesvollzug, in Regierungsbehörden, Unternehmen und Rechtsanwaltskanzleien etc. tätig sind, vertrauen bereits auf die AccessData Software-Lösungen. Weitere Informationen unter www. accessdata.com .

Weitere Informationen:
AccessData Group
Nicole Reid
International Marketing Manager
1 Bedford Street
3rd Floor
London
E-Mail: nreid@accessdata.com
Internet: www.accessdata.com
Ansprechpartner (in Deutschland):
Abdeslam Afras
Director, EMEA
 India
E-Mail: aafras@accessdata.com
PR-Agentur:
Sprengel
 Partner GmbH
Nisterstraße 3
D-56472 Nisterau
 www.sprengel-pr.com
Ansprechpartner:
Olaf Heckmann
Marius Schenkelberg
Tel.: +49 (0)26 61-91 26 0-0
Fax: +49 (0)26 61-91 26 0-29
E-Mail: ms@sprengel-pr.com
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=578384" width="1" height="1">

Pressekontakt

AccessData Group

84042 Lindon, UT

nreid@accessdata.com

Firmenkontakt

AccessData Group

84042 Lindon, UT

nreid@accessdata.com

Weitere Informationen finden sich auf unserer Homepage