Hack In the Box: Pentests im Krankehaus

Medizinischer Notfall

Kai Kunschke

Ausnahmsweise einmal nicht um Pflege, sondern um einen Notstand ganz anderer Art ging es bei der HITB: Betroffen war der „Patient" Krankenhaus, der beängstigende sicherheitstechnische Gebrechen aufweist.

Vom 12. bis 13. April fand zum neunten Mal die Hackerkonferenz Hack In The Box (HITB) Amsterdam statt. Veranstaltungsort war das Grand Hotel Krasnapolsky unweit des berühmt-berüchtigten Rotlichtviertels von Amsterdam. Auf insgesamt drei Tracks verteilten sich unzählige spannende Vorträge, wobei der thematisch gemischte CommSec-Track sogar für die interessierte Öffentlichkeit frei zugänglich war. Ergänzt wurden die Vortragsreihen durch den Track „HITB Labs" mit fünf Workshops, etwa zu den Themen Software-defined Radio oder Jailbreaken und Analyse der Datenstrukturen im iOS-Kernel.

Malware = Malware?

Auffällig war, dass alle drei Keynotes von Frauen gehalten wurden. Neben Jennifer Leggio von Flashpoint und Amber Baldet, bis vor Kurzem bei JPMorgan, berichtete die inzwischen bei Intel angestellte Marion Marschalek in der Eröffnungskeynote aus ihrer beruflichen Praxis in der Security-Branche. Ihrer Erfahrung als Malware-Analystin nach ist Schadsoftware, die als „Advanced Persistent Threat" (APT) gelabelt wird, oftmals gar nicht ausgefeilter, komplexer oder gar schädlicher als „normale" Malware.

Marschalek ist auch Gründerin von „Blackhoodie", einem kostenlosen Reverse-Engineering-Bootcamp für Frauen. Es sei wichtig, betonte sie, Räume zu schaffen, in denen sich die Teilnehmerinnen wohlfühlen. Denn sich wohlzufühlen ist eine Voraussetzung, um kreativ sein zu können. Das ist in der männerdominierten IT-Welt für viele Frauen nicht der Fall, weshalb sie dieses Camp ausschließlich für Frauen gegründet hat.

Die Blackhoodie-Absolventin Maria „Azeria" Markstedter leitete den Workshop „From Zero to ARM Assembly Bind Shellcode". Nach einer kurzen Einführung in die wichtigsten Konzepte der Assembler-Programmierung und in einige ARM-Instruktionen wurden die Teilnehmer in die Lage versetzt, ein kompaktes Programm zu schreiben, das den Linux-Systemcall *execve("/bin/sh", 0, 0)* absetzt. Dazu wurde der besonders kompakte Thumb-Mode des ARM-Prozessors verwendet, um Null-Bytes zu vermeiden. Auch andere Maßnahmen zur Vermeidung von Null-Bytes wurden vorgestellt. Nach und nach wurde der Shellcode um Netzwerkoperationen erweitert, bis man schließlich eine Reverse-Shell und eine Bind-Shell erhielt. Den fabrizierten Code konnten die Teilnehmer auf einem emulierten Raspberry Pi dann auch gleich ausprobieren.

Beunruhigend und aufregend zugleich war der Vortrag „Somebody Call a Doctor: Hacking a Hospital for Fun and Profit" der israelischen Sicherheitsexperten Asaf Cohen und Ofir Kamil. Die beiden Pentester teilten ihre abenteuerlichen Erfahrungen aus der Sicherheitsüberprüfung eines Krankenhauses. Schon beim frühmorgendlichen Kaffeeholen in der Krankenhaus-Cafeteria entdeckten die beiden einen offenen WLAN-Access-Point, der Zugang zum komplett flachen Krankenhausnetzwerk ermöglichte. Alternativ hätte man auch einen der unzähligen frei zugänglichen RJ45-Ports an den Wänden nutzen können, denn eine Network Access Control gab es nicht.

Sicherheits-GAU vernetzte Geräte

Die Pentester entschieden sich aber lieber für ein Kiosk-System, das sie per Explorer-Kontextmenü übernahmen. Natürlich lief die Anwendung im Kontext des Windows-Administrators. Von hier aus verschafften sie sich Zugangsrechte zum Domänen-Admin. Um über einen offenen VNC-Port (Virtual Network Computing) auf einen Computertomografen (CT) oder per Telnet mit Standardpasswörtern auf ein EKG-Gerät zuzugreifen, brauchten sie diese Rechte freilich nicht. Besonders gruselig war, dass die Pentester Zugang zu einem Webinterface der Steuerungskomponente von Gaspumpen erlangten. Geschützt war dieser Zugang nur durch das Passwort „1". Der Vortrag hat bei den Zuhörern den Wunsch, Krankenhäusern möglichst fernzubleiben, weiter verstärkt.

Die Websecurity-Experten Lukas Weichselbaum und Michele Spagnuolo von Google gaben Einblick in moderne Sicherheitsmechanismen für Webanwendungen. Vor allem zum richtigen Einsatz der Content-Security-Policy-Header (CSP) konnten die beiden wertvolle Hinweise und einen Ausblick auf CSP 3 liefern. So sollten Admins eine Whitelist-basierte CS-Policy durch Nonce- oder Hash-basierte Policies ablösen und gar nicht erst versuchen, das Abfließen von Daten per CSP zu verhindern. Google schützt rund 50 % seines Datenverkehrs per CSP.

(ur@ix.de)