ERNW Newsletter 23 / April 2007

Liebe Partner, liebe Kollegen,

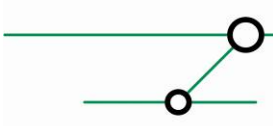
willkommen zur 23ten Ausgabe des ERNW-Newsletters mit dem Thema:

Neuigkeiten aus dem Untergrund
Ein Bericht der Blackhat Europe 2008

Version 1.0 vom 10. April 2007

von: Michael Thumann, mthumann@ernw.de

INHALTSVERZEICHNIS



1 EINLEITUNG

Am 27. März war es wieder soweit: zwei Tage lang wurden auf der Blackhat Europe in Amsterdam die neusten Ergebnisse aus der Hacker Szene präsentiert. Mit dabei war auch wieder ERNW mit einem Vortrag über „Hacking SecondLife“ (http://www.blackhat.com/html/bh-europe-08/bh-eu-08-archives.html#Thumann). Neben dem eigenen Vortrag gab es aber auch reichlich Gelegenheit, sich über die Ergebnisse anderer Experten zu informieren und mit Bekannten aus der Szene die aktuellen Trends zu diskutieren. Die Information aus erster Hand, möchten wir an unsere Newsletter Abonnenten weitergeben und haben daher die wichtigsten und interessantesten Vorträge hier zusammen gefasst.

2 CLIENT-SIDE ATTACKS VON PETKO PETKOV

Dieser Vortrag stellt die verschiedensten Angriffsvektoren gegen Client-System vor. Dabei fokussierte Petko Petkov sich auf Client Applikationen, die auf jeden Client zu finden sind und demonstrierte für jede Applikation einen erfolgreichen Angriff. Betroffen waren die Applikationen Firefox, Internet Explorer, Skype, Quicktime, Flash Player, SecondLife Viewer, Citrix Client und Java Runtime sowie einige Internet Dienste wie z. B. GMail. Es wurde eindrucksvoll klargestellt, dass Angriffe gegen den Client zu den Security Trends 2008 gehören.

3 ATTACKING ANTIVIRUS VON FENG XUE

Auch der Vortrag von Feng Xue beschäftigt sich mit Angriffen gegen den Client, allerdings wird hier die Antivirensoftware als Angriffsvektor benutzt, also eine Software, die eigentlich den Client schützen soll. Feng Xue zeigte einige Angriffe gegen bekannte Antivirensoftware, die in erster Linie Softwarefehler innerhalb der Applikation ausnutzten und durch Versenden eines präparierten Dateianhangs in die Antivirensoftware eingeschleust wurden. Das Ergebnis war größtenteils eine totale Kompromittierung des Client Systems.

4 CISCO IOS FORENSICS VON FELIX LINDNER

Felix Lindner, bekannt als FX, stellte seine neuesten Forschungsergebnisse aus dem Cisco Umfeld vor. Es handelt sich dabei um ein Werkzeug zur forensischen Analyse von Cisco Geräten. Voraussetzung ist eine entsprechende Konfiguration der Cisco Geräte, um alle Informationen auch auf einem zentralen Server abzulegen. Diese Informationen werden dann auf Hinweise eines möglichen Hacker Angriffs untersucht und mittels eines Reports dargestellt. Diesem Vortrag kommt unter anderem auch deshalb eine besondere Bedeutung zu, da das Potential für erfolgreiche Angriffe gegen Netzwerkgeräte meistens sehr unterschätzt wird und bisher keine Werkzeuge zur Verfügung standen, um hier eine forensische Analyse zu betreiben.

5 EXPLOITING VULNERABILITIES IN MEDIA SOFTWARE VON DAVID THIEL

David Thiel’s Ansatz Clients zu attackieren, fokussiert sich auf Media Files, also MP3/MP4 Dateien, die zugehörigen ID Tags, aber auch andere Formate, sowie Audio und Video Dateien. Im Zuge der Research Arbeit wurde ein Fuzzer entwickelt, der Test Files für verschiedene Media Player erzeugt und mit Hilfe dieser Tests wurden mehrere verbreitete Media Player untersucht. Am Ende der Tests konnten in allen Produkten (von VLC bis iTunes) Security Bugs gefunden werden. Da auch in den Firmen sehr viel mit Media Dateien gearbeitet wird bzw. solche Dateien auch von den Mitarbeitern aus dem Internet heruntergeladen werden können, zeigt auch dieser Vortrag das hohe Gefährdungspotential der Clients im Unternehmen.

6 LDAP Injection von Chema Alonso und Jose Parada Gimeno

Neben den allgemein bekannten Injection Angriffen wie SQL Injection und Cross-Site Scripting ist auch LDAP Injection seit ca. 2 Jahren in der Security Community bekannt. In diesem Vortrag wurde aber erstmalig der allgemeinen Öffentlichkeit dieser Angriff vorgestellt und auch in verschiedenen praktischen Beispielen demonstriert. Betroffen sind in erster Linie komplexe Webanwendungen, die mit Authentifizierungsservern zusammenarbeiten und das Protokoll LDAP benutzen. Dabei dürfte es sich aber um eine durchaus große Menge handeln, da LDAP sowohl in homogenen Windows Umgebungen eingesetzt wird, wie auch mit OpenLDAP im Open Source Umfeld. Zusätzlich muss noch beachtet werden, dass gerade in großen Umgebungen verschiedene User Datenbanken in übergeordneten Meta Directories zusammengefasst werden, um die User Verwaltung zentral managen zu können. Die Kommunikation mit diesen Meta Directories erfolgt üblicherweise mittels LDAP.

7 Intercepting Mobile Phone/GSM Traffic von David Hulton

Mobiltelefone werden heute von fast jedem benutzt, ohne sich großartig über die Sicherheit Gedanken zu machen. Die Ursache dafür ist hauptsächlich darin zu suchen, dass technische Detailinformationen, wie z. B. eingesetzte Verschlüsselung oder Ortbarkeit von Mobiltelefonen kaum an die Öffentlichkeit dringen, aber auch dass das technische Equipment um GSM Verkehr mitlesen zu können sehr teuer ist (> $100.000,--). Eine Gruppe von Security Researchern hat jetzt nach einem langjährigen Projekt seine Ergebnisse vorgestellt. Dies beinhaltet die genutzte technische Ausstattung (ca. $1.000,--), sowie auch eine Darstellung der vorgefundenen „Zustände“. In der Praxis wurde demonstriert wie völlig problemlos die SIM-Karten ID mitgelesen werden konnte, dabei handelt es sich um ein Weltweit eindeutiges Identifizierungsmerkmal des Kunden. Weiterhin wurde der Verschlüsselungsalgorithmus der Daten geknackt, so dass ein Mitlesen der geführten Gespräche verhältnismäßig einfach möglich ist. Bei vielen Providern wird aber auch gar keine Verschlüsselung benutzt, so dass die Daten im Klartext über die Luft übertragen werden. Das bedeutet, dass mit einem Kostenaufwand von ca. $1.000,-- und etwas Know-How, Mobiltelefongespräche von jedermann abgehört werden können.

8 Weiterführende Infos

Sollten wir mit diesen kleinen Zusammenfassungen Ihr Interesse geweckt haben, so erhalten Sie weiterführende Informationen auf der Webseite der Blackhat Europe 2008 Konferenz:
http://www.blackhat.com/html/bh-europe-08/bh-eu-08-archives.html

Die Folien, sowie auch Whitepaper zu den einzelnen vorgestellten Vorträgen, finden Sie unter den folgenden Links:

1. Client-side attacks von Petko Petkov
   http://www.blackhat.com/html/bh-europe-08/bh-eu-08-archives.html#Petkov
2. Atacking Antivirus von Feng Xue
   http://www.blackhat.com/html/bh-europe-08/bh-eu-08-archives.html#Sowhat
3. Cisco IOS Forensics von Felix Lindner
   http://www.blackhat.com/html/bh-europe-08/bh-eu-08-archives.html#Lindner
4. Exploiting Vulnerabilities in Media Software von David Thiel
   http://www.blackhat.com/html/bh-europe-08/bh-eu-08-archives.html#Thiel
5. LDAP Injection von Chema Alonso und Jose Parada Gimeno
   http://www.blackhat.com/html/bh-europe-08/bh-eu-08-archives.html#Alonso
6. Intercepting Mobile Phone/GSM Traffic von David Hulton
   http://www.blackhat.com/html/bh-europe-08/bh-eu-08-archives.html#HultonD

9 ZUSAMMENFASSUNG

Die Vorträge der aktuellen Security Konferenzen zeigen für das Jahr 2008 eindeutige Trends, welche Security Themen für die Unternehmen relevant werden. Das große Thema schlechthin ist Client Security in jeglicher Ausprägung, ob die Angriffe dabei über Antivirensoftware, Multimedia Files, Messaging oder Browser durchgeführt werden, spielt erstmal eine untergeordnete Rolle. Auch das Thema Mobile Security gewinnt immer mehr an Bedeutung, da es mit den aktuellen Techniken und Produkten immer schwieriger wird, die Authentizität, Integrität und Vertraulichkeit der mobilen Daten zu schützen.

Mit freundlichen Grüßen,

[Michael Thumann].

ERNW GmbH
Michael Thumann
Senior Security Consultant

ERNW Enno Rey Netzwerke GmbH
Breslauer Str. 28
69124 Heidelberg
Tel. +49 6221 480390
Fax +49 6221 419008
www.ernw.de