it-defense 2005

Von jvm

cirosec GmbH
Ferdinand-Braun-Straße 3
74074 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

Inhalt

1. Vorwort

In Köln fand vom 26.1. bis zum 28.1. der IT-Sicherheits-Kongress IT-Defense statt. Motto des von cirosec und dpunkt.verlag veranstalteten Kongresses war: "Meet the IT-Security wizards".

Eröffnung der Konferenz

Die (leider immer) aktuelle Thematik und die hochkarätigen Referenten sorgten dafür, dass das auf 200 Teilnehmer begrenzte Treffen trotz des hohen Preises (ab 995,- EUR) komplett ausgebucht war.

Wer immer die Gelegenheit hat, seine Firma zu überzeugen, dass er (oder auch sie, Grüße an die Dame vom Bundesamt für Informationstechnologie) zu dieser Tagung muss (privat ist es doch arg teuer) - macht es! Wann hat man schon mal die Gelegenheit, den Programmierer von Nessus, den Schöpfer des Sleuth-KIts, den Erfinder der Proxy-FW sowie unzählige andere Fachleute zu treffen und sich mit ihnen auszutauschen? Oder mit Clifford Stoll (ja, exakt, der allererste "Hackerjäger" und Autor von "Kuckucksei") über Gott und die Welt, Kinder, Gesellschaft und Computersicherheit zu reden. Für diejenigen, die an der Thematik interessiert sind, aber nicht teilnehmen konnten, stelle ich hier einige Vorträge des zweiten Tages (Mittwoch, 26.1.2005) vor.

2. Die Vorträge

Marcus Ranum nach dem Vortrag

Nach kurzer Begrüßung durch Stefan Strobel lautete der erste Vortrag von Marcus J. Ranum "Die Dynamik der Verschiedenheit in der Computersicherheit". Ranum beschäftigte sich intensiv mit dem häufig geäußertem Vorwurf, dass Monokulturen wie zum Beispiel der hohe Anteil von Microsoft-Betriebssystemen und Anwendungen mit Ursächlich an der desolaten Sicherheitslage in der IT seien. Ranum vertritt die These, dass wir noch nicht von einer Monokultur sprechen können, da unter anderem Desktops unterschiedlich konfiguriert sein können, unterschiedliche Programme nutzen etc. In größeren Installationen (sei es in Firmen oder komplexeren häuslichen Installationen) wird die vermeintliche Monokultur noch stärker aufgeweicht durch komplexe Kombinationen von Routern, Firewalls, Desktops etc.

Bedrohlicher als das Streben eines Anbieters nach Monopolbildung findet er den Wunsch vieler Systemadministratoren nach einfacher, zentraler Administration, bedingt durch möglichst gleiche Hardware bzw. Software auf den verschiedenen Rechnern.

Trotz aller Vorteile, die so etwas natürlich hat, wie zum Beispiel

einfachere Administration, weniger aufwändiges Benutzertraining usw. macht man sich durch zentrale Administration auch zentral angreifbar.

Mit schönen, griffigen Beispielen fegte Ranum en passant zwei weitere, gerne benutzte Schreckgespenster hinweg: die Dominotheorie (kaskadierende Fehler) und die Cyberwar-Theorie.

Bezüglich der ersten Theorie führte er aus, dass Menschen sich zwar gerne aufregen, aber keineswegs direkt der dritte Weltkrieg ausbricht, selbst wenn alle Computer weltweit ausfallen würden.

Cyberwar scheitert heutzutage seiner Meinung nach an mangelnder Technologie und an fehlenden Ressourcen. Wenn man sich Beispielsweise vorstellt, dass ein Team von Experten gebildet wird, dieses für alle möglichen Systeme des Gegners X geschult wird, sogar eine gravierende Lücke entdeckt, die sonst noch niemand gefunden hat, zu geeigneter Zeit zuschlagen will - um dann entsetzt festzustellen, dass dieser Exploit vorgestern auf Bugtraq veröffentlicht wurde und der Bug gefixt ist.

Ranum sieht die Ursachen für viele Sicherheitsprobleme eher im mitunter seltsamen Verhalten der Industrie und der User. Bei den Herstellern gibt es eine gefährliche Hingabe zu riskanten Praktiken wie zum Beispiel WLan, VoIP, Bluetooth und so weiter - in allen Fällen fielen die gravierenden Sicherheitslücken erst nach Markteinführung auf. Seltsam auch das Verhalten von Usern, die Software von Firmen kaufen, die bekannt sind für ihre Sicherheitslücken. Oder diejenigen, die unsichere Produkte nutzen, obwohl es sicherere Alternativen gibt (ja, damit sind u.a. IE und Outlook gemeint).

Der Schluss seines Vortrages betrachtete die für Sicherheit aufzuwendenden Kosten - nachdem man schon für die Software, die es abzusichern gilt, ein große Menge Geld ausgegeben hat.

Ebenso interessant wie der Vortrag (und seine Vortragsart) waren die Statements von Ranum in kleiner Runde - darum hier ein paar der schönsten/provokantesten ohne weiteren Kommentar:

- einige Entwickler scheinen ihre eigenen Programme teilweise nicht mehr zu verstehen - wie sonst ist zu erklären, dass Bugfixing teilweise so lange braucht
- Linux entwickelt sich in eine Richtung, wo "es" nie hinwollte - kommerziell, Business. Seitdem Red Hat, SUSE etc. teure Unternehmenslizenzen anbieten, zücken auch Firmen die Scheckbücher, die Linux vorher belächelt haben - verrückt.
- Immer komplexere Programme, immer mehr Gadgets, Sachen, die keiner braucht, machen Programme immer schwieriger zu warten und angreifbarer.
- Firmen kaufen Software, die nicht funktioniert - gerne auch mehrmals hintereinander beim gleichen Anbieter - WARUM?


Tobias Klein

Der Vortrag von David Litchfield fiel am Mittwoch leider aus, dafür referierte Tobias Klein über "Advanced Exploiting". Tobias ist unter anderem Autor zweier sehr empfehlenswerter Bücher (Buffer Overflows und Format-String-Schwachstellen: Funktionsweise, Exploits und Gegenmaßnahmen, 663 Seiten, Dpunkt Verlag, ISBN 3898641929; sowie Linux-Sicherheit. Security mit Open-Source-Software - Grundlagen und Praxis, 750 Seiten, Dpunkt Verlag, ISBN: 3932588045) und sorgte mit seinem Vortrag für ungläubiges Staunen.

Nachdem er die Hauptursache für Systemeinbrüche, Memory Corruption Vulnerabilities (zum Beispiel Buffer Overflows, Format-String-Overflows etc.) kurz vorgestellt hatte, kam er zur generischen Funktionsweise der Exploits. Um die Kontrolle über den Programmfluss zu erhalten, muss ein Exploit seinen (malicious) Code hineinbringen. Hierfür wurden Begrifflichkeiten aus der Militärtechnik entliehen, nämlich Injection Vector und Payload. Stellen wir uns also einen Exploit als Marschflugkörper vor, dessen Nutzlast der bösartige Code ist.

Normale Exploits greifen bekannte Sicherheitslücken an, um Kontrolle über ein Programm zu erlangen und andere Befehle in diesem Kontext auszuführen. Um sich nun vor Bedrohungen zu schützen, installiert man häufig eine Firewall, durchaus auch in der ausgeklügelten Version der Stateful/Deep Protocol/Packet Inspection. Zusätzlich werden noch IDS (Intrusion Detection System) und IPS (Intrusion Prevention System) installiert, um im Falle eines Einbruchs wenigstens etwas davon mitzubekommen und Beweise zu sichern. Zu guter Letzt wird alles noch per chroot dichtgemacht.

All dies soll dazu beitragen, dass man auch bei neueren Exploits relativ sicher ist. Denn gerade in umfangreicheren Systemen sind Patches nicht mal eben in fünf Minuten eingespielt - schon mal gar nicht, wenn man vorher testen muss, ob die verwendete Software auch nach dem Patchen noch funktioniert.

Fassen wir kurz zusammen, was es zu meistern gilt: Hineinkommen in ein gesichertes System, Firewall überwinden, keinen Alarm auslösen, keine Spuren hinterlassen, Root-Rechte erlangen, Dateien hoch- und herunterladen, verändern, lesen, Host hopping.

Viele geben sich nun der verhängnisvollen Illusion hin, dass die oben genannten vorgeschalteten Sicherheitsmechanismen das Ausnutzen von Exploits eigentlich unmöglich machen. Tobias zeigte dem Auditorium recht deutlich, dass dem nicht so ist.

Er hat ein Programm namens Gen1 Zecke (Gen1 steht für Generation 1) entwickelt, das er auf folgendes Setting losließ:

Apache (mit der Buffer-Overflow-Schwachstelle CAN-2002-0656)
CheckPoint FW R55W mit Deep Protocol Inspection

Die Zecke marschierte durch die Firewall, nutzte den Buffer-Overflow aus, startete eíne Shell, lud einen weiteren Exploit, machte sich zum root und

war Herr des Systems. Das alles mit netter Menuführung auf Konsolenebene. Was zeigten die Logs der Firewall: nichts. Was enthüllten uns forensische Tools: ebenfalls nichts, keine Datei war geändert.

Denn das Programm von Tobias nutzte keines der vorhandenen Programme, sondern hatte diese in Form von Syscalls nachgebildet (via Syscall Redirection). Es lief einzig und allein im Hauptspeicher als geforkter Prozess des Apache und war damit sehr sicher vor Entdeckungen. Glücklicherweise gibt es dieses Programm nirgends zum Herunterladen; aber es macht deutlich, dass Abwehrstrategien auf Netzwerkebene nicht ausreichend sind und eher trügerische Sicherheit vorgaukeln.

Den folgenden Vortrag von Stefan Strobel verpasste ich leider, da ich mich mit Clifford Stoll "verlaberte".

In Brian Carriers Beitrag wurde sehr intensiv (und sehr schnell, er war zehn Minuten vor dem Zeitplan fertig) auf die verschiedenen forensischen Methoden zur Untersuchung "gehackter" Systeme eingegangen, insbesondere auf die Unterschiede zwischen Live- & Dead-Analyse. Anhand des Beispiels eines Root-Kits illustrierte Brian die verschiedenen Stufen der Live-Analyse, sowohl mit kommerziellen Tools als auch mit freien Tools wie zum Beispiel mit dem von ihm entwickelten Sleuth-Kit.

War schon Brians Vortrag stark theoretisch ausgerichtet, fügte Gregoire Ribordy dem noch eine gehörige Portion Quantenphysik hinzu. Sein Thema war die Quantenkryptographie, genauer gesagt der abhörsichere Austausch der Verschlüsselungs-Schlüssel mittels Quantenphysik. Konkret geschieht dies mittels Photonen, einem Glasfaserkabel, etwas Polarisierung sowie dem ein oder anderen Photonengatter. Vereinfacht gesagt kann man mit entsprechend polarisierten Photonen binäre Informationen übertragen, wobei 1 Photon = 1 Bit. Da jeder Versuch des Abhörens den Zustand des Photons verändern würde (wir erinnern uns kurz: Quantenphysik ist grob gesagt die Heisenbergsche Unschärferelation und Schrödingers Katze, käme es nicht mehr als valides Bit im "Zählgatter" an. Noch ist diese Form des Schlüsselaustausches jedoch recht teuer und aufgrund der optischen Eigenschaften der Glasfaser auf ca. 100 km Reichweite beschränkt.

Man möge mir verzeihen, dass ich die letzten beiden Vorträge so kurz behandelt habe - sie waren jedoch so voll mit Informationen, dass eine angemessene Wiedergabe mehrere Seiten füllen würde.

Ein Vortrag kam aber noch - mit dessen Referenten hatte ich mich Mittags schon verquatscht (und dafür das Mittagessen im Hilton sausen lassen!). Daher wusste ich, dass Cliff zum einen ewig keinen Vortrag über Sicherheitsthemen gehalten hatte und nicht vorbereitet war.


Clifford Stoll

Dann betrat Dr. Stoll die Bühne. Für die jüngeren Leser: er war derjenige, der zuerst einen bzw. mehrere Hacker aufspürte, verfolgte und dingfest machte (nachzulesen in dem wunderbaren Buch "Kuckucksei", teilweise nachzusehen in dem schrecklichen Film "23"), das Ganze Ende der 80er, als es das Internet in seiner heutigen Form noch gar nicht gab.

Cliff bezeichnet sich selber als old-fashioned und lehnt

daher selbstredend die Benutzung von Powerpoint ab. Er benutzte die Folien von vor 20 Jahren auf dem Overheadprojektor. Seine Vortragsart entspricht etwa dem Gebaren von Otto auf Speed mit dem Humor der kompletten Monty-Phyton-Gruppe.

Inhaltlich ging es überwiegend um die Geschehnisse des "KGB-Hacks", der sozialen Verantwortung auch von Security-Experten etc. Mehr zu seinen Ideen und Ansichten gibt es in dem Artikel, der auch das Interview mit Cliff enthält.

Man möge sich kurz vorstellen: der Kongress lief seit 9:00 Uhr, alle Vorträge waren enorm mit Informationen gespickt, bis auf den Vortrag von Tobias waren alle in Englisch (und verlangten somit etwas mehr Konzentration) und es war inzwischen schon 17:00 Uhr. Bis dahin bestand der Saal aus über 200 sehr Interessierten, aber doch inzwischen leicht erschöpften Teilnehmern. Ab dann war Müdigkeit und Erschöpfung kein Problem mehr - dafür taten sich andere auf. Menschen bekamen vor Lachen kaum noch Luft, sahen nichts mehr, weil ihnen die Augen tränten vom Lachen...

Noch nie habe ich es so bedauert, keinen Camcorder zu besitzen. Nach eineinhalb Stunden musste man leider langsam zum Ende kommen, um 18:30 Uhr gab es "standing ovations" für Clifford Stoll.

3. Fazit

Mein Fazit: Ein absolut lohnenswerter Kongress, der viele Anregungen gab, der perfekt organisiert war und tolle Referenten hatte. Mein Dank auch an das Team der Veranstalter, insbesondere Frau Seigerschmidt für den netten Kontakt und die "Interviewvermittlung".

Pro-linux.de, 07.02.05