13. deutscher EDV-Gerichtstag Saarbrücken 2004

Sitzung des Arbeitskreises
„Datensicherheit als Herausforderung in der Kanzlei und in Unternehmen“
Universität Saarbrücken, Gebäude 16, Hörsaal 117,
Donnerstag, den 16. September 2004, 13 Uhr 00 bis 14 Uhr 40

Die Sitzung wurde um 13 Uhr 00 durch den Vorsitzenden des Arbeitskreises, Herrn Vorsitzenden Richter am Bundespatentgericht Dr. rer. nat. Wolfgang Tauchert vor ca. 25 teilnehmenden Personen eröffnet. Der Vorsitzende stellte kurz den Referenten, Herrn Toralv Dirro, Fa. Network Associates GmbH, Hamburg vor und gab eine kurze Einführung in die Thematik des Vortrags.

Im Zentrum des Vortrags steht die Gefährdung der Funktion von Computersystemen durch Angriffe von außen, die den Verlust, die Ausspähung oder die Manipulation von Daten, die Schädigung des Systems oder Störungen seiner Funktionsabläufe und nicht zuletzt die missbräuchliche Fremdsteuerung der gesamten systeminternen Datenaustausch- und Kommunikationswege zur Folge haben können. Diese Angriffe haben unter den Begriffen „Viren“, „Würmer“ und „Trojaner“ in die computerfachliche Umgangssprache Eingang gefunden.

Der Referent zeigte zu Eingang seines Vortrags auf, daß die Weiterentwicklung der Angriffsmethoden mit der Weiterentwicklung der Systemtechnologie Schritt hält. Dominierten anfangs noch Viren, die im Bootsektor der Datenträger angesiedelt waren, wurden diese schon bald durch mit dem Aufkommen elektronischer Fernkommunikation durch Makroviren und „Mass Mails“ abgelöst. Seit 2001 sind im Netz sogenannte „Blended Threats“ im Umlauf, die unter Verwendung von Hackertechnologien gezielt Sicherheitslücken in den Systemen aufspüren und ausnutzen. Hierzu gehört z. B. der auch in den Tagesmedien bekannt gewordene Wurm „Sasser“. Eine weitere Evolution und Ausbreitung der Angriffstechnologien ist durch die steigende Bedeutung kabelloser Datenkommunikation, insbesondere in Verbindung mit Mobiltelephonen und Laptops zu erwarten. Die fortschreitende technologische Entwicklung hat zur Folge, daß die noch zur Verfügung stehende Reaktionszeit gegen neuartige Angriffe sich immer weiter verkürzt.

Zuverlässigste Komplizin der sogenannten Massmails ist oft die menschliche Neugier, die dazu führt, daß Anhänge auch unbekannter e-mails unbedacht geöffnet werden, wodurch sich Viren verbreiten können.

Bei Würmern ist festzuhalten, daß diese bislang nur Kollateralschäden angerichtet haben, die darin bestanden, daß ganze Rechner lahmgelegt wurden bzw. pausenlos herauf- und heruntergefahren wurden.

Bei den „blended threats“ versagt die konventionelle Virenabwehrsoftware, da hier einfach bereits vorgegebene Sicherheitslücken im System ausgenutzt werden.

Besonders gefährlich sind die sogenannten „Trojaner“. Diese können dazu führen, daß das System unbemerkt durch den Hacker ferngesteuert werden kann und weitere Systeme infiziert werden. Im Bereich der Rechtsanwendung und Rechtspflege erscheint dies besonders folgenschwer, da neben der Funktionssabotage auch Authentizität und Vertraulichkeit der Daten nach einem Trojanerbefall nicht mehr gewährleistet sind. Es ist auf diese Weise sogar möglich, den PC am Arbeitsplatz bei vorhandenem Mikrophon zum Abhören und bei vorhandener Videokamera zur optischen Ausspähung zu verwenden.

Ähnliche Wirkung kann auch durch missbräuchliche Verwendung von Security tools erzielt werden.

Es ist ein weitverbreiteter Irrtum, anzunehmen, diese Gefahren könnten durch firewalls abgewehrt werden oder es verbliebe im Falle eines bevorstehenden Angriffs noch genügend Reaktionszeit. Auch reine „Intrusion detection“-Systeme geben keinen Schutz, sie zeigen einen Angriff lediglich an, wehren ihn aber nicht ab und sind somit lediglich einer „stillen Alarmanlage“ vergleichbar. Es ist auch ein Irrtum, anzunehmen, daß UNIX-Systeme nicht von dieser Problematik betroffen wären.

Ziel jeder Abwehrstrategie muß es sein, das Zeitfenster der Systemverwundbarkeit möglichst gering zu halten. Abwehrstrategien erscheinen nur dann als erfolgversprechend, wenn diese mehrere Ansätze miteinander verbinden, wobei eine vollständige Sicherheit nicht erreicht werden kann. Darüber hinaus ist ein zeitnahes Management erforderlich, um den Eintritt von Schäden zu verhindern bzw. die Folgen zu minimieren.

Neben der Beibehaltung der konventionellen Virenabwehr müssen die Vorhandenen „Intrusion detection“-Systeme zu „intrusion prevention“-Systemen weiterentwickelt

werden. Hierbei ist eine reaktive Komponente erforderlich, die nach Art einer Mustererkennung über eine Bibliothek der Eigenschaften bereits bekannter Angriffe verfügt. Spricht diese Mustererkennung im System an, wird die Operation blockiert und der Systemadministrator wird informiert. Neuartige Angriffe werden durch die Implementierung von Verhaltensmaßregeln ermittelt. Durch diese werden Aufrufe und Operationen festgelegt, die für den bestimmungsgemäßen Betrieb des Systems nicht erforderlich sind, es wird eine Liste potentiell erwünschter Software erstellt, bestimmte Querverbindungen innerhalb des Systems, die nicht zwingend notwendig sind, werden ebenfalls verboten. Hierdurch kann das Risiko gesenkt und das Zeitfenster der Verwundbarkeit verkleinert werden. Erschwert werden diese Strategien durch die Auflockerung der Systeme, wie sie durch die zunehmend steigenden Computerfunktionen von Mobiltelephonen und durch die nicht mehr leitergebundene elektronische Kommunikation bewirkt werden.

Nach dem Ende des Vortrags um ca. 14 Uhr 15 schloß sich noch eine Diskussion an. Auf entsprechende Frage wurde festgehalten, daß genaue Zahlen und kriminologische Daten über diese Angriffe derzeit nicht bekannt sind, es ist von einem hohen Dunkelfeld auszugehen. Ein geringeres Risiko bei der Verwendung von Linux besteht nicht, ebenso auch nicht bei Einsatz von open-source-Software.

Im Verlauf der Diskussion wurde die Empfehlung gegeben, Anhänge von e-mails mit dem Suffix „exe“ grundsätzlich nicht zu öffnen, auf nicht notwendige Funktionen bei Mobiltelephonen sollte verzichtet werden, letztere können ein leicht zugängliches Eingangstor für solche Angriffe darstellen.

Kaiserslautern, den 16.09.2004

Dr. rer. nat. Jan Fritz Geiger
Rechtsanwalt und Diplomphysiker
Universität Saarbrücken und
RAe Scheidel & Scheidel, Kaiserslautern