security zone newsletter
PLATTFORM FÜR INFORMATIONSSICHERHEIT

EU-Projekt NoAH zur Früherkennung und Bekämpfung von neuen Cyberattacken

Aktuelle Schutzmassnahmen für IT-Infrastrukturen sind oft machtlos gegen Cy-berattacken, die eine bisher unbekannte Schwachstelle ausnutzen. Oft kommen sie auch mit bekannten Angriffen in neuem Kleid nicht gut zurecht. Das EU Projekt NoAH soll helfen, diese Lücke zu schliessen.

Bernhard Tellenbach

Doktorand am Institut für Technische Informatik und Kommunikationsnetze der ETH Zürich

Wie verheerend die Auswirkungen eines Angriffs auf die IT Infrastruktur von Firmen und Privatpersonen sein können, stellten die Cyberattacken durch Würmer wie Blaster, SQL-Slammer oder Sobig unter Beweis. Trotz verbesserten Schutzmassnahmen und rascherer Behebung von Sicherheitslücken bleibt das Risiko durch Cyberattacken bestehen.
Schutzmassnahmen wie Intrusion Detection Systeme oder Virenscanner verwenden zur Erkennung einer Cyberattacke meist Signaturen, die manuell oder halbautomatisch erstellt werden. Da diese Art der Signaturgenerierung zeitintensiv ist, muss der Nutzen solcher Signaturen bei sich schnell verbreitenden Würmern in Frage gestellt werden. Der Slammer-Wurm infizierte zum Beispiel 90% aller verwundbaren Hosts in nur 10 Minuten [1].

Das EU Projekt NoAH

Im April 2005 startete das bis März 2008 laufende EU-Projekt NoAH (Network of Affined Honeypots) [2]. Das Ziel des Projektes ist, einen Beitrag zur Früherkennung und Bekämpfung von bekannten und neuen Cyberattacken zu leisten. Dieses Ziel soll mit Hilfe eines Netzwerkes von kooperierenden Honeypots erreicht werden. Das Projekt unternimmt die notwendigen vorbereitenden Arbeiten zur Realisierung einer entsprechenden europäischen Infrastruktur. Die Infrastruktur soll ein breites Spektrum an Informationen an interessierte Partner liefern. Die Zielgruppe mit Fokus auf Security Emergency Response Teams, nationale Cyber-Security-Institutionen, IT-Sicherheitsverantwortliche sowie Forscher im Bereich IT Sicherheit ist sicherlich gross.

Honeypots

Ein Honeypot ist ein System, das als Falle für nicht legitimierte Benutzer und Angreifer fungieren soll. Weil meist keine legitime Nutzung des Honeypots vorgesehen ist, kann jegliche Nutzung als illegitim klassiert werden. Die Aufzeichnung der Aktivitäten auf dem Honeypot ermöglicht es somit, Informationen über Angreifer und Angriffstechniken zu sammeln. Ein Beispiel: Eine Firma konfiguriert einen Computer identisch zu ihrem Fileserver. Der Computer wird aber nicht als Fileserver genutzt. Den legitimen Benutzern ist dies bekannt. Sucht und Attackiert nun ein nicht legitimer Benutzer den Fileserver, kann er den echten Fileserver nicht vom Honeypot unterscheiden. Wählt er sein Ziel zufällig aus, landet er mit 50%-iger Wahrscheinlichkeit auf dem Honeypot.

Sicherheitslücke Honeypot

Wie jedes andere System innerhalb einer IT Infrastruktur stellt auch ein Honeypot ein potentiell verwundbares System dar. Meist wird ein Honeypot gar

absichtlich exponiert, um ein interessanteres Ziel für Angreifer darzustellen. So wird z.B. oft auf den Einsatz einer Firewall verzichtet, oder es wird bewusst Software mit bekannten Sicherheitslücken verwendet. Falls nun ein Angreifer die Kontrolle über einen Honeypot innerhalb eines Firmennetzes erlangt, ergeben sich prinzipiell folgende drei Risiken:

1. Der Honeypot wird zum Sammeln von Informationen im Firmennetz missbraucht.
2. Der Honeypot wird für weitere Angriffe auf das Firmennetz verwendet.
3. Der Honeypot wird für Angriffe auf andere IT-Infrastrukturen eingesetzt. Für angerichtete Schäden kann der Honeypot-Betreiber möglicherweise haftbar gemacht werden.

Um eine gute Abdeckung des europäischen Teils des Internets mit Honeypots zu erreichen, müssen diese auch in Firmennetzen platziert werden können. Hierfür ist sicherlich die Minimierung der obigen Risiken bei gleichzeitig hoher Attraktivität des Honeypots erforderlich. Heutzutage gibt es unterschiedliche Ansätze, dieses Ziel zu erreichen. Die zugrunde liegenden Prinzipien sind Abschottung, Simulation und Schutz durch Detektion und Eindämmung.

Sicherheit: Abschottung

In die Kategorie Abschottung fällt z.B. die logische und/oder physikalische Trennung des Firmennetzes vom Honeypot. Dies verhindert, dass der Honeypot als Tor in das Firmennetz verwendet werden kann. Eine andere Methode ist, den Honeypot hinter eine Firewall zu platzieren, die alle vom Honeypot initiierten Verbindungen blockiert (auch Reverse-Firewall genannt). Dadurch sind vom Honeypot ausgehende Angriffe auf Ziele jenseits der Firewall sowie das aktive Sammeln von Informationen über die Firewall-Grenze hinweg nicht mehr möglich. Der Honeypot könnte somit Informationen nur noch passiv (durch Abhören seiner Kommunikationsleitungen) sammeln. Zudem muss der Angreifer diese Informationen über eine von aussen initiierte Verbindung abholen.

Sicherheit: Simulation

Eine weitere Möglichkeit, die Risiken stark zu vermindern, ist, die erreichbaren Dienste nur zu simulieren. Beispielsweise kann man anstelle von einem echten Windows-XP-System ein Linux System mit HoneyD [3] verwenden. HoneyD gibt sich dann als Windows XP System aus und simuliert ein Set von ausgewählten Diensten. Der Nachteil dieser Methode ist, dass die Funktionalität komplexer Dienste nur eingeschränkt möglich ist. Überprüft ein Angreifer ein System auf solche Einschränkungen, kann er einen Honeypot als solchen erkennen. Neben HoneyD stellen spezialisierte Simulatoren wie MultiPot [4] interessante Ansätze dar.

Sicherheit: Eindämmung

Die Kategorie Schutz durch Detektion und Eindämmung ist von grosser Bedeutung, wenn kein simuliertes, sondern ein reales System als Honeypot dient. Zwei Ansätze, welche die Übernahme eines Systems durch das Einschleusen und Ausführen von fremdem Code verhindern, sind TaintCheck [5] und Argos [6]. Ihr Funktionsprinzip ist das folgende: Alle vom Angreifer an den Honeypot übertragenen Daten werden markiert. Dadurch kann deren Weg durch den Speicher verfolgt werden. Falls der Honeypot versuchen sollte, markierte Daten auszuführen, wird ein Alarm generiert. Anschliessend kann die Ausführung, z.B. zwecks Verfolgung der Absichten des Angreifers, zugelassen oder geblockt werden.

Fazit

Momentan gibt es verschiedene viel versprechende Ansätze, einen Honeypot so abzusichern, dass sein Einsatz das Risiko für die IT-Infrastruktur einer Firma nicht erhöht. Die Hauptaufgabe des NoAH-Projektes wird nun sein, die vorhandenen Ansätze weiterzuentwickeln und in ein Gesamtsystem zu integrieren.

[1] Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S., and Weaver, N. Inside the Slammer worm. IEEE Security and Privacy 1, 4 (Jul. 2003).
[2] NoAH project Webseite www.fp6-noah.org
[3] The Honeyd Virtual Honeypot www.honeyd.org
[4] MultiPot http://labs.idefense.com/
[5] TaintCheck http://www.ece.cmu.edu/~jnewsome/docs/taintcheck.pdf
[6] Argos http://www.few.vu.nl/~porto/argos/