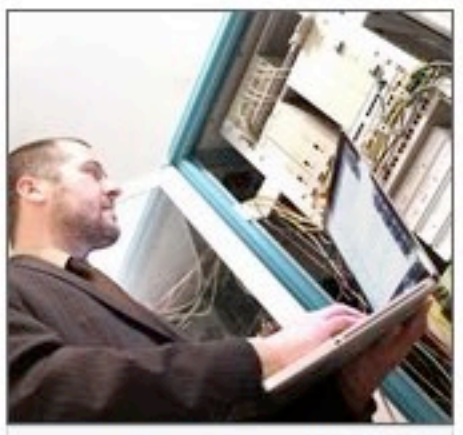
04.Jan.2011 Artikel versenden | Drucken

Nethinks: Automatisierter Schutz – auch vor dem Unbekannten



um-werbephotographie (Uli Mayer)

Bisher können interne Störungen in der IT-Landschaft mittels Software schnell lokalisiert und behoben werden. Mit dem neuen Frühwarnsystem sollen künftig auch unbekannte externe Cyber-Attacken auf Netzwerke effektiv abgewehrt werden können.

Forschen gemeinsam an einer neuen Sicherheitssoftware (v. l.): Uwe Bergmann, Geschäftsführer Nethings und Professor Dr. Hans-Ulrich Bühler, Projektleiter im Fachbereich Angewandte Informatik der Hochschule Fulda.

Die Hochschule Fulda und das Fuldaer Unternehmen Nethinks entwickeln eine neue Software zur IT-Sicherheit in einem gemeinsamen Forschungsprojekt.

Vorsorge ist besser als Nachsorge. Die alte Volksweisheit gilt insbesondere im Zeitalter der Digitalisierung. Denn: „Sicher ist, dass das Internet nicht sicher ist - und zwar schon per Definition. Einen 100-prozentigen Schutz davor, dass Daten mitgelesen und verändert werden können, gibt es auch durch Firewalls oder Spamfilter bisher nicht, sondern höchstens durch das Ziehen des Steckers." Darin sind sich Professor Dr. Hans-Ulrich Bühler, Leiter der Arbeitsgruppe IT-Sicherheit des Fachbereichs Angewandte Informatik (AI) der Hochschule Fulda, und Uwe Bergmann, Geschäftsführer der Nethinks, einig.

Teil 2: Forschung für drei Jahre gesichert

Heute lässt sich mit Cyberkriminalität viel Geld verdienen und entsprechend groß ist die Kreativität der Angreifer, um Sicherheitsvorkehrungen zu umgehen. Ein Bollwerk gegen schadhafte Software wie Viren oder Trojaner taugt nur so lange, bis Hacker die Funktionsweise kennen und mit neuen Schadcodes dagegenhalten. Genau an diesem Punkt setzt das aktuelle Forschungsprojekt an, an dem der Fachbereich AI gemeinsam mit Nethings in den kommenden drei Jahren arbeitet. „Die Entwicklung eines Sicherheitsanalysetools zur automatisierten Netzwerküberwachung" ist Titel und Zielsetzung gleichermaßen.

„Die zunehmende Digitalisierung von Informationen und die Vernetzung sämtlicher elektronischer Geräte verlangen ein höheres Maß an IT-Sicherheit, denn im gleichen Maße steigen die Angriffsszenarien - vor allem auf Unternehmernetzwerke - aus dem Internet heraus. IT-Sicherheit muss in jeder Unternehmensstruktur fest verankert sein - das ist die Basis für wirtschaftlichen Erfolg", weiß Professor Dr. Hans-Ulrich Bühler aus Erfahrung. Die Idee, einen Automatismus zu entwickeln, der mehr Sicherheit bringt, sei nicht neu, der aktuelle Forschungsansatz dagegen schon.

Teil 3: Aus Monet entsteht Sec-Monet

Basis ist das von Nethinks entwickelte Monitoring-Werkzeug Monet, mit dem sich interne Störungen lokalisieren und beheben lassen. „Diese vorhandenen Daten aus internen IT-Netzwerken möchten wir zu einer Art Frühwarnsystem für bisher unbekannte Cyber-Attacken weiterentwickeln, die von externen Angreifern zum Beispiel mit dem Ziel der Wirtschaftsspionage ausgeführt werden. Aus Monet entsteht dabei Sec-Monet", so Bühler weiter.

„Eine effektive Technik zur Prävention von externen Angriffen gibt es noch nicht, denn es entstehen täglich mehrere Tausend Varianten von Schadsoftware. Bisher können Schutzprogramme wie ein handelsüblicher Virenscanner erst dann greifen, wenn die Funktionsweise einer neuen Schadsoftware bekannt ist. Wir erforschen dagegen eine Lösung, die es erlaubt, schon vorab zu reagieren- auch ohne das neue Angriffsszenario zu kennen", beschreibt Uwe Bergmann die Zielsetzung.

Teil 4: Nutzen für mittelständige und große Unternehmen

Wichtige Grundlage für die Forschung ist das Wissen um veränderte Aktivitäten innerhalb eines Netzwerks vor und während einer Offensive von außen. Verlängerte Ladezeiten von Rechnern oder der unerklärbare Anstieg von Serveraktivitäten sind potenzielle Indikatoren dafür, dass eine Gefahr droht. „Wir erkennen dabei gewisse Muster und entwickeln daraus automatisierte Schutzmechanismen", erklärt Bühler.

Positive Forschungsergebnisse bringen vor allem einen hohen Nutzen für mittelständische und große Unternehmen, die über eine komplexe IT-Infrastruktur verfügen. Aber auch private User können profitieren, denn: „Die Grundlagen unserer Forschungsergebnisse werden in einem zweiten Schritt auch in Anwendungen für private Nutzer zur Verfügung stehen. Außerdem profitieren private Nutzer indirekt, wenn es uns zum Beispiel gelingt, in Behörden oder Kreditinstituten gespeicherte personenbezogene Daten so gut zu schützen, dass sie garantiert nicht in falsche Hände geraten können", betont Bergmann.

Teil 5: Zum Hochschulforschungsprojekt

Das Projekt wird mit über 400 000 Euro gefördert - knapp zwei Drittel davon stellt das Bundesministerium für Bildung und Forschung zur Verfügung, ein Drittel trägt die Nethings. Zwei Mitarbeiter sind an der Hochschule Fulda beschäftigt, einer davon in einer Doktorandenstelle, hinzukommen zwei Tutoren. Ebenso sind zwei Mitarbeiter der Nethings ins Forschungsprojekt eingebunden. Zwischen allen Beteiligten erfolgt ein kontinuierlicher Austausch - digital und persönlich. Unterstützt wird das Projekt durch forschungsnahe Institutionen und weitere Unternehmen, die zum Beispiel zugesagt haben, nach Abschluss der Forschung die Effektivität von Sec-Monet in der Praxis zu testen.

Anne Lauer

Know-how IP-TK-Anlagen

Fachwissen zum Thema **VoIP-Migration**:

VoIP für Klein- und Mittelständler ▸ **mehr ...**

Alles über den Microsoft Lync Server 2010 ▸ **mehr ...**

IP-Telefone als Alleskönner ▸ **mehr ...**

Wenn TDM- und NGN-Welt aufeinander prallen ▸ **mehr ...**

Brücken zum Mobilfunk ▸ **mehr ...**

Bedrohung für Asterisk-TK-Anlagen ▸ **mehr ...**

TK-Anlagen auf dem IP-Pfad ▸ **mehr ...**

Wartungsverträge im Zeitalter von IP ▸ **mehr ...**