Gegen die dunkle Seite des Internets

Hans-Joachim Hof bewegt sich auf der dunklen Seite des Internets. Im Cyberspace spürt der Professor für sichere Softwaresysteme an der Fakultät für Informatik und Mathematik Hacker auf, jagt Spam-Versender und sichert Netzwerke von Unternehmen. Dazu entwickeln der IT-Spezialist und sein Team in der MuSe – Munich IT Security Research Group vor allem Software, die die Nutzung des Internets sicherer macht.

„Ich war selbst ein Hacker", schmunzelt Hof. „Aber ich war ein White-Head-Hacker", erläutert er. „Das heißt, ich wurde von Firmen beauftragt, deren IT-Umgebung anzugreifen und mit meinen Erkenntnissen sicherer zu machen." IT-Sicherheit blieb ein großes Thema für Hof, jetzt an der Hochschule München eher aus forschender Sicht.

„Eine Fremdnutzung durch die Hacker könnte zum Beispiel eine Überlast des eigenen Servers zur Folge haben", erläutert der Professor. Ein Hacker kann unter anderem den gekaperten Rechner nutzen, um Spam-Mails zu verschicken. Doch nicht nur Firmenrechner sind von solchen Zugriffen betroffen, auch der eigene PC ist es. „Bringen Sie einen neuen Windows-Rechner ins Internet, so ist er nach einer Viertelstunde weltweit bekannt", schildert Hof die prekäre Lage.

Ein Mittel gegen Spam-Mails auf heimischen Computern haben Hof und sein Team bereits entwickelt: Die IT-Spezialisten haben ein System programmiert, mit dem alle betroffenen Rechner in einer konzertierten Aktion eine Rückantwort an durch Spam beworbene Webshops schicken. „Das erzeugt bei den Betreibern hohe Datenströme und damit Kosten", erklärt der IT-Experte. „So wird es unrentabel, für Werbung auf Spams zu setzen." Dass so ein Abwehrsystem für den Programmierer nicht risikofrei ist, hat sich bei der Firma Blue Frog gezeigt. Deren MitarbeiterInnen programmierten ein ähnliches System, das allerdings zentral von den Servern der Firma organisiert und koordiniert wurde. Sie waren massiven Drohungen der Spamsender ausgesetzt. „Aus diesem Grund haben wir entschieden, die Idee so zu erweitern, dass wir die Software auf vielen Rechnern von Benutzern laufen lassen, damit sie nicht einfach ‚ausgeschaltet' wird", erklärt Hof.

Neben Spam-Mails terrorisieren Viren die Internetnutzer. Was den heimischen PCs widerfahren kann, passiert auch bei komplexen Rechnersystemen in Unternehmen. „Um Software sicherer zu machen", sagt Hof, „muss man schon bei ihrer Entwicklung sorgfältiger als bisher arbeiten und mehr auf Softwarequalität achten." Ein häufig benutzter, agiler Software-Entwicklungsprozess ist Scrum. Hier ändern sich Anforderungen an die Software oft noch während der Programmierung, so dass auch die Sicherheitsmaßnahmen ständig an neue Randbedingungen angepasst werden müssen – für Sicherheits-Experten ein Alptraum. In einem Projekt, das Hof mit Unterstützung des Bayerischen Staatsministeriums für Bildung und Kultus, Wissenschaft und Kunst durchführt, untersuchten die IT-Spezialisten, wie man diesen Prozess optimieren kann. Als Ergebnis dieses Projekts entstand „Secure Scrum", eine Erweiterung von Scrum zur Entwicklung von sicherer Software. Neben Softwareentwicklungsprozessen wurden in der MuSe auch verschiedene Werkzeuge zum Testen von Sicherheit entwickelt, welche die Erstellung sicherer Software unterstützen.

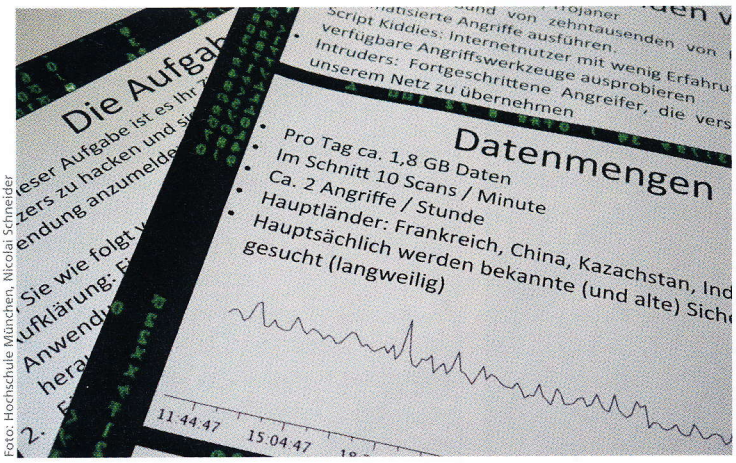

Foto: Hochschule München, Nicolai Schneider

Übersicht über Hackerangriffe.

Hier liegt ein besonderer Schwerpunkt auf Embedded Devices, da durch neue Anwendungsdomänen wie z.B. Industrie 4.0 und Connected Car mit vermehrten Angriffen auf diese Geräte zu rechnen ist.

Neben Computern bieten auch Smartphones und Handys eine Gelegenheit für Cyberkriminelle, um in Netzwerke einzudringen. Hof und seine Mitarbeiter entwickeln Schutzsoftware für Firmennetzwerke, in deren Umfeld private Mobiltelefone oder Tablets verwendet werden. Solche Geräte nutzen zum Beispiel firmeneigene Internetanwendungen oder Apps und sind direkt mit dem Unternehmen verbunden. „Wir wollen die Bedrohung von Firmennetzwerken durch diese Geräte minimieren", sagt der Wissenschaftler.

Hans-Joachim Hof sieht die Zukunft der IT-Sicherheit nicht rosig: „Die Veröffentlichungen von Edward Snowden haben gezeigt, dass das, was möglich ist, auch getan wird. Neue Anwendungsdomänen wie z. B. Industrie 4.0 oder Connected Car bieten vielfältige neue Angriffsmöglichkeiten, zum Teil mit gravierenden Auswirkungen." Seiner Meinung nach wäre auch eine politische Reaktion notwendig. „Wir brauchen mehr europäische bzw. deutsche Software im Bereich Sicherheit, und wir benötigen auch eine eigene Hardware-Plattform. Helfen würde es schon, wenn es weiterreichende Haftungsregeln für die Hersteller von Software gäbe, so dass im Schadensfall nach einem Angriff der Hersteller der Software eintreten muss. So würden für Softwarehersteller Anreize existieren, mehr in Softwarequalität speziell im Bereich IT-Sicherheit zu investieren. Existierende Initiativen wie z. B. IT Security Made in Germany gehen nicht weit genug."

Thorsten Naeser
Hochschule München

INFOS

Weitere Informationen unter
http://muse.bayern