3 FRAGEN AN… RALF BENZMÜLLER, HEAD OF G DATA SECURITYLABS

1. Herr Benzmüller, welche aktuellen Entwicklungen gibt es im Zusammenhang mit Virenschutz und Cybercrime?

Am weitesten verbreitet sind Adware und potenziell unerwünschte Programme. Sie machen ca. ein Drittel aller Infektionen aus. Die Einblendung von Werbebannern ist lukrativ für Kriminelle, wird aber von den meisten Nutzern gar nicht als schädlich wahrgenommen. Das macht sie zu einem rentablen Geschäft.

Die auffälligste Entwicklung ist der Bereich Ransomware. Immer neue Spielarten von Verschlüsselungstrojanern erscheinen, und die Vorgehensweise variiert. Es gibt Ransomware, die alle möglichen Dateien im privaten Bereich verschlüsselt. Andere Varianten sind auf Unternehmen ausgelegt und verbreiten sich im lokalen Netzwerk. Manche verschlüsseln die Webseite und ermöglichen den Besuchern nur noch den Zugang zu einer Seite mit der Lösegeldforderung. Andere verschlüsseln den Zugang zum häuslichen Netzwerkspeicher (NAS). Oder der Zugang zum Internet wird deaktiviert und mit einem Lösegeld belegt.

In den letzten 15 bis 20 Jahren hat sich eine florierende Cybercrime-Ökonomie etabliert, deren Umsätze schon lange die des Drogenhandels übersteigen. Das erbeutete Geld wird in neue Angriffe investiert, deren Planung und Umsetzung immer öfter professionell betrieben wird. Mittlerweile gibt es kaum noch einen Bereich in unserem Alltag, in dem keine Rechner eingesetzt werden. Entsprechend gravierender sind die Folgen von Angriffen. Deshalb bekommt der Schutz vor Angriffen auf Rechner eine immer wichtigere Rolle in der Gesellschaft.

2. Vor welcher Art von Cybercrime kann ein Virenschutz Unternehmen schützen?

Ein klassischer Virenschutz ist dazu konzipiert, automatisierte Angriffe zu erkennen und abzuwehren, insbesondere wenn sie massenhaft auftreten. Mit seinen vielen Komponenten schützt ein Virenschutz vor Infektionen über die klassischen Wege E-Mail, manipulierte Webseiten oder über lokale Netzwerke und USB-Datenträger. Ein guter Virenschutz verhindert, dass ein Rechner mit Adware infiziert wird, Bestandteil eines Botnetzes wird oder dass sensible Daten verloren gehen. Spezielle dynamische Erkennungsverfahren schützen auch gegen Angriffe über Sicherheitslücken und bewachen das Online-Konto während des Online-Bankings.

Diesen Gefahren sind sowohl Nutzer von privaten Computern ausgesetzt als auch User im Unternehmensumfeld. In Unternehmen sind weitere Funktionen wichtig, wie z.B. Backups, Patch-Management und Mobile Device Management.

3. Wie können Unternehmen sich, neben dem Schutz durch ein Antivirus-Programm, am effektivsten vor einer Attacke schützen?

Eine Antivirensoftware ist eine wichtige Basiskomponente für ein Virenschutzkonzept. Für eine umfassende Abwehr von Angriffen reicht das aber nicht aus. Virenschutz ist nur dann effektiv, wenn er in ein umfassendes Schutzkonzept eingebettet ist. Das beginnt mit der Zugangskontrolle zu Räumen und Gebäuden, setzt sich fort mit der Auswahl von Hardware, Betriebssystem und Software. Dann geht es weiter mit der sauberen Trennung von Netzwerksegmenten und der Vergabe von Zugangsrechten für Nutzer. Für besonders sensible Bereiche sollten zusätzliche Erkennungs- und Schutztechnologien eingesetzt werden. Eine besondere Rolle kommt den Mitarbeitern zu. Ohne deren Mitwirkung lässt sich kein Schutzkonzept sinnvoll umsetzen. Es ist daher unumgänglich, bei den Mitarbeitern durch regelmäßige Schulungen ein gesundes Sicherheitsbewusstsein aufzubauen.