9. November 2005

Hintergrundinformation

Rekordmonat für Computerviren – Vorbeugender Schutz schlägt bloßes Reagieren

Signatur-basierte Verfahren geraten bei der Abwehr von IT-Schädlingen ins Hintertreffen

Gleich mehrere Hersteller von Antiviren-Programmen meldeten in Sachen neu entdeckter Viren, Würmer und anderer Malware für den vergangenen Monat Rekordzahlen. Wurden schon in den Vormonaten regelmäßig mehr als 1.000 neue IT-Schädlinge registriert, stieg die Zahl im Oktober auf fast 1.700 an. Jede einzelne Variante muss so schnell wie möglich erfasst und analysiert, die Antiviren-Software ständig mit den aktuellen Signaturen aktualisiert werden. Ein Verfahren, das mit der rasant steigenden Zahl der Viren und der Geschwindigkeit ihrer Veränderung den Sicherheitsanforderungen von Unternehmen und Computernutzern nicht immer gerecht werden kann.

X-Force: Jagd nach Schwachstellen

Einen anderen Ansatz verfolgt die X-Force, eine hundertköpfige Forschungstruppe des Anbieters von Sicherheitslösungen Internet Security Systems (ISS). Im Labor ist das Team ständig auf der Suche nach Schwachstellen und möglichen Angriffspunkten in Software, Datenbanken, Betriebs- und Netzwerksystemen. Entdeckt die X-Force eine Schwachstelle, wird der Hersteller darüber in Kenntnis gesetzt und aufgefordert, einen entsprechenden Patch zu liefern. Innerhalb kürzester Zeit, bei kritischen Ereignissen sofort, werden präventive Updates für die ISS-Produkte bereitgestellt. Durch dieses Verfahren sind die bei Kunden zum Einsatz kommenden Lösungen automatisch gegen mögliche Angriffe auf die Schwachstelle geschützt. ISS spricht in diesem Zusammenhang von „Virtual Patching“. Mehr als die Hälfte aller weltweit

entdeckten kritischen Sicherheitslücken geht auf die Arbeit der X-Force zurück.

Beispiel Zotob: Vier Monate vor dem Angriff geschützt

Ein Beispiel aus diesem Jahr belegt die Effizienz der X-Force und der präventiven Sicherheitsstrategie von ISS: Bereits am 13. April deckt die X-Force die Schwachstelle im Windows Plug & Play-Dienst auf und aktualisiert die ISS-Produkte mittels Virtual Patch. Erst am 8. August veröffentlicht Microsoft die Schwachstelle und stellt einen Patch bereit – wenige Tage später greift Zotob an und verursacht unter anderem in großen US-Amerikanischen Medienhäusern wie CNN und der New York Times Systemausfälle. ISS-Kunden waren zu diesem Zeitpunkt schon seit vier Monaten gegen Zotob und alle seine Varianten geschützt. Signaturbasierte Verfahren können nur den Angriff abwarten und müssen auf jede Variante einer Malware neu reagieren.

Kriminelle Strategien

Die schnellsten Anbieter von Antiviren-Produkten schaffen den signaturbasierten Schutz gegen einen Schädling in etwa acht Stunden nach seiner Entdeckung. Kriminelle Virenprogrammierer reagieren darauf mittlerweile mit „Short Span Attacks“ und „Serial Variant Attacks“. Angreifer sind also beispielsweise nur wenige Stunden lang aktiv oder werden in kurzen Intervallen in unterschiedlichen Varianten losgelassen. Diese Strategien machen es den Herstellern von Antiviren-Lösungen immer schwerer, auf die Angriffsflut zu reagieren. Gegen präventive Schwachstellensuche und Virtual Patches dagegen haben derartige Angriffe kaum eine Chance.

Ca. 3.176 Zeichen bei durchschnittlich 65 Anschlägen pro Zeile (inklusive Leerzeichen)