

Antivirensoftware – Wegbereiter für Datendiebe

Wenn der Wächter zum Türöffner wird

Thierry Zoller, Senior Security Engineer bei N.Runs

Virens Scanner halten technische und wirtschaftliche Fallstricke bereit, die vielen Unternehmen nicht bewusst sind. Mehrere hundert Schwachstellen haben Sicherheitsexperten in den vergangenen Monaten in allen gängigen Antivirenlösungen aufgespürt. Das Ergebnis: Entgegen ihrer eigentlichen Schutzfunktion öffnen die Produkte Angreifern die Tür und ermöglichen es ihnen, in Firmennetzwerke einzudringen und diese mit Schadcode zu infiltrieren. Somit stellt die Platzierung von AV-Software an zentralen Stellen in der IT-Infrastruktur ein potenzielles Sicherheitsrisiko dar.

Die Attacke auf das Netzwerk erfolgt manchmal quasi durch die Hintertür – das Schlupfloch für die Datendiebe ist der Virens Scanner, dessen eigentliche Aufgabe es ist, Schaden abzuwehren. Das Problem ist hausgemacht: Die von dem IT-Sicherheitsspezialisten N.Runs durchgeführten Tests haben gezeigt, dass jeder der am Markt befindlichen Virens Scanner gleich mehrere hochkritische Schwachstellen aufweist. Dies untermauern auch Erhebungen der Universität Michigan. Laut deren Statistik wurden zwischen 2002 und 2005 insgesamt 50 Advisories zu Sicherheitslücken in Antiviren-Produkten veröffentlicht. Zwischen 2005 und 2007 steigerte sich diese Zahl immens – um 340 Prozent auf 170 Advisories. Auf der diesjährigen Blackhat-Europe-Konferenz wurden außerdem Untersuchungen präsentiert, die besagen, dass in den vergangenen vier Jahren 164 Sicherheitslücken aufgetaucht sind.

Das SANS-Institut hat AV-Engines als Einfallstor in ihre Top-20 der Sicherheitsrisiken aufgenommen.

Offenes Scheunentor

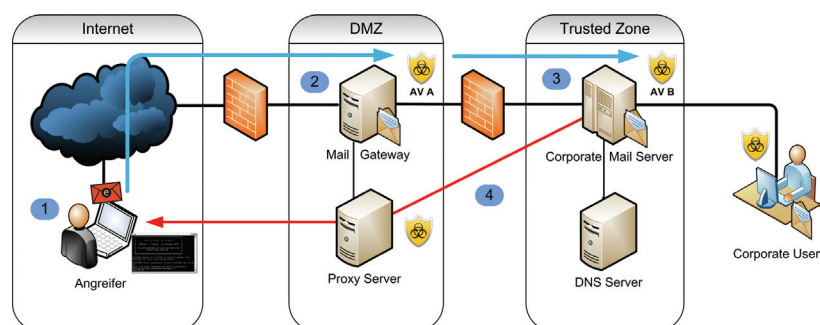
Die Schwachstellen ebnen den Weg für Denial-of-Service-Attacken (DoS) und ermöglichen es, Schädlinge an der Sicherheitslösung vorbei ins Netzwerk zu schleusen und sogar Exploitcode auszuführen. So lässt sich zum Beispiel direkt durch das Ausnutzen der AV-Komponente der E-Mail-Verkehr einsehen oder die An-

tivirensoftware zum Absturz bringen und damit gegebenenfalls ein Ausfall der gesamten E-Mail-Infrastruktur auslösen. Der Schutz der AV-Lösung kann auch komplett umgangen werden, so dass Viren oder Malware zum End-User gelangen. Das Fazit: Die Produkte erlauben genau das, wovor sie eigentlich schützen sollen.

Verhängnis „Parsing“

Als eine der Hauptursachen für den beschriebenen Effekt gilt das so genannte Parsing. Die Parsing-Engine ist unverzichtbarer Bestandteil einer jeden AV-Software. Das Prinzip funktioniert wie folgt: Virens Scanner müssen möglichst viele Schädlinge erkennen und somit eine hohe Anzahl an Dateiformaten verstehen und verarbeiten. Um binäre Formate interpretieren zu können, muss eine Applikation die entsprechenden Dateien in Blöcke und Strukturen aufteilen. Dieses Zerlegen von Daten in analysierbare Einzelteile wird als Parsing bezeichnet. Hierbei werden Speicherblöcke reserviert, um Daten aus der Datei in diese Blöcke zu kopieren. Einer der besonders anfälligen Vorgänge hierbei besteht darin, dass Datenblöcke ohne Kontrolle des Inhaltes und häufig auch ohne Kontrolle der Länge in den Speicher kopiert werden und dabei in vielen Fällen zu angreifbaren Schwachstellen führen. Außerdem entstehen durch Fehlannahmen beim Parsen Konstellationen, die es ermöglichen, Programmcode einzuschleusen und auszuführen.

Da Antivirenlösungen bewegliche Ziele sind, ändern sich ständig ihre



Funktionen und die Anzahl der zu erkennenden Formate. Je mehr Formate eine solche Software verstehen muss, desto mehr und häufiger muss diese „parsen“ – und desto höher ist die Fehlerwahrscheinlichkeit. Beispielsweise erkannte Kaspersky im Jahr 2006 nahezu 2000 Formate, 2007 erhöhte sich die Anzahl auf 3000. Hinzu kommt, dass die von den Herstellern erwartete schnelle Reaktionszeit hinsichtlich der Bedrohungen zum Qualitätsverlust des Codes beiträgt. Kurzum: Je mehr Parsing stattfindet, umso höher ist zwar die Erkennungsrate und der Schutz vor Schadsoftware, desto größer wird jedoch gleichzeitig die Angriffsfläche und die Antivirenlösung wird selbst zur Zielscheibe.

Eine weitere Krux in diesem Zusammenhang ist die Tatsache, dass Unternehmen oft mehrere AV-Engines einsetzen, damit alle geschäftskritischen Server und Clients durch Software, die mit den höchsten Rechten ausgestattet ist, umfassend geschützt sind. Dadurch erhöht sich die Anfälligkeit noch einmal dramatisch. Das Paradoxe dabei ist: Kommt eine Vielzahl unterschiedlicher AV-Engines zum Einsatz, vergrößert sich die Gesamtangriffsfläche und somit die Wahrscheinlichkeit, dass der Angreifer leichtes Spiel hat.

Angriffsszenario

Jede Antivirensoftware weist bei isolierter Betrachtung bereits potenzielle Schwachstellen auf. Entdeckt der Angreifer nur einen einzigen Fehler in der Parsing-Engine eines eingesetzten Virenschanners, kann er hierdurch die Kontrolle über den Server erlangen, den die E-Mail gerade durchläuft. Steht der Server im Herzen des Unternehmens, kann er dem Angreifer Zugriff auf alle Daten des Mailserver geben. Hierauf finden sich oft die Daten der gesamten elektronischen Kommunikation des Unternehmens. Außerdem wird es dem Angreifer somit möglich, sich Zugang zu anderen Segmenten des Netzes zu

verschaffen und „Trust Relationships“ auszunutzen. Da AV-Software mit hohen Zugriffsrechten laufen muss, ergeben sich höchst attraktive Angriffsziele. So ist der Angreifer beispielsweise durch das Verschieben einer E-Mail mit präpariertem ZIP-Anhang in der Lage, diverse Manipulationen an internen Systemen vorzunehmen, auf denen sich Antivirensoftware im Einsatz befindet.

Schutzwall für die Antivirenlösung

Der IT-Sicherheitsspezialist N.Runs hat über 800 Schwachstellen aufgedeckt und gemeldet. Hiervon wurden einige entfernt, aber die meisten existieren nach wie vor. Grund dafür ist unter anderem, dass es bis zu zwei Jahre dauern kann, bis Produkt-Patches ausgeliefert werden, die die Sicherheitslücken beseitigen, da AV-Engines in vielen Produkten zum Einsatz kommen und der Entwicklungsaufwand sehr hoch ist.

Parsing als eine der Hauptursachen lässt sich nicht umgehen, da dieser Vorgang als Erkennungsmechanismus bei der Bekämpfung digitaler Schädlinge unverzichtbar ist. Die Lösung ist daher die Einbettung der existierenden AV-Lösungen in eine hochsichere Architektur, die unter anderem erfolgreiche Angriffe auf die gesamte AV-Infrastruktur verhindert und durch Mehrfach-Scanning gleichzeitig die Virenerkennungsrate herkömmlicher Antivirenprogramme sowie den Schutz vor Malware erhöht.

Diese so genannte Aps-AV-Lösung wurde einem BSL-Klasse-4-Virenlabor (Biosafety Level) nachempfunden, wobei Kontroll-, Abschottungs- und Vernichtungsmechanismen nachgebildet werden. Hierbei unterteilt sich die Architektur in die drei Schutzzonen „Front-End“, „Distribution“ und „Execution“, welche über Firewalls (Paketfilter) separiert werden. Die Kommunikation der verschiedenen Systeme über diese Sicherheits-schichten hinweg erfolgt über ein

speziell für die Sicherheitsbedürfnisse der Architektur entwickeltes Protokoll.

Das Systemdesign basiert nicht auf unmittelbaren Vertrauensbeziehungen. Alle Daten werden derartig kryptographisch gesichert transportiert, dass nur die für den Betrieb der Lösung erforderlichen Informationen übertragen werden können. Bei der Implementierung wurde strikt dafür Sorge getragen, dass die zu untersuchenden Daten zu keiner Zeit auf bekannte Viren-Signaturen hin inspektiert oder durch Parsing interpretiert werden, bevor sie in die abgesicherte Ausführungsumgebung gelangen. Die verwundbaren AV-Engines kommen erst im Execution Environment – das zusätzlich zum Sicherheitsfaktor des gehärteten Hochsicherheitsbetriebsystems über keinerlei Netzwerkschnittstellen verfügt – zum Zug und überprüfen den Mail-Anhang auf Schadcode. Stellt das System eine Anomalie fest, wird die abgeschottete Umgebungsamt Betriebssystem komplett gelöscht und der Vorgang als Angriff auf das AV-Produkt markiert. Die Distribution Engine gibt dem Mail-Server dann entweder grünes Licht oder veranlasst das Blockieren der E-Mail. Außerdem wird der Vorfall zentral geloggt und gemeldet.

Aps-AV 3-Tier-Architektur

Gemeinsam mit Antivirensoftware-Anbietern als Technologiepartner und durch Aspekte wie Zentralisierung werden Funktionalität, Hochverfügbarkeit und Sicherheit der AV-Lösungen gewährleistet, so dass die Kontrollübernahme zum Beispiel über den Mailserver oder den dahinter liegenden AV-Client verhindert werden kann. Eine derartige Technik richtet sich insbesondere an Großunternehmen, Konzerne und Provider mit hohem Sicherheitsbedarf. Angriffe im Rahmen gezielter Industrie- und Wirtschaftsspionage sowie Manipulation und Kompromittierung der E-Mail-Infrastruktur sind damit chancenlos. ■