

Virens Scanner machen Angreifern den Weg ins Netzwerk frei

n.runs warnt:

Antivirensoftware – vom Wächter zum Spion

Oberursel, 23. Juni 2008 – Rund 800 Schwachstellen haben Spezialisten der n.runs AG sowie andere Sicherheitsexperten in den vergangenen Monaten in Virenschutzlösungen aufgespürt. Das Fazit: Entgegen ihrer eigentlichen Funktion öffnen die Produkte Angreifern die Tür und ermöglichen es ihnen, in Firmennetzwerke einzudringen und diese mit Schadcode zu verseuchen. Die Platzierung von Antivirensoftware an zentralen Stellen im Unternehmen stellt demnach ein hohes Sicherheitsrisiko dar. Die n.runs AG reagiert auf diese Tatsache mit dem eigens entwickelten System aps-AV – eine Lösung, die die komplette E-Mail- und Anti-Virus-Infrastruktur absichert und alle Angriffe von außen unterbindet.

Die von dem Consulting-Unternehmen und Lösungsentwickler n.runs durchgeführten Tests haben gezeigt, dass jeder der am Markt befindlichen Virens Scanner gleich mehrere hochkritische Schwachstellen aufwies. Diese ebnet den Weg für Denial of Service(DoS)-Attacken und ermöglichen es, Schädlinge an der Sicherheitslösung vorbei ins Netzwerk zu schleusen und sogar Schadcode auszuführen. Somit erlauben Antivirenlösungen genau das, wovon sie eigentlich schützen sollen.

Als eine der Hauptursachen für diesen Bumerang-Effekt konnte n.runs das so genannte Parsing ausmachen. Das Prinzip funktioniert wie folgt: Virens Scanner müssen möglichst viele Schädlinge erkennen und somit eine hohe Anzahl an Dateiformaten verstehen und verarbeiten. Um die Formate interpretieren zu können, muss eine Applikation die entsprechende Datei in Blöcke und Strukturen aufteilen. Dieses Zerlegen von Daten in analysierbare Einzelteile wird als Parsing bezeichnet. Durch Fehlannahmen beim Parsen entstehen Konstellationen, die es ermöglichen, Programmcode einzuschleusen und zur Ausführung zu bringen. Ferner trägt die von den Herstellern erwartete schnelle Reaktionszeit hinsichtlich Bedrohungen zum Qualitätsverlust der Codes bei. 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 Ziel-

scheibe. Gezielte Industrie- und Wirtschaftsspionage sowie das Unterbrechen der gesamten E-Mail-Kommunikation sind nur zwei der möglichen Folgen.

Bollwerk für die Antivirenlösung

Damit der Virens Scanner nicht zum Einfallstor im Netzwerk wird und Angreifer nicht die Kontrolle übernehmen können, hat n.runs das Application Protection System – Anti-Virus (aps-AV) auf den Markt gebracht. Die eigens konzipierte und entwickelte Lösung komplettiert die IT-Sicherheitsinfrastruktur von Unternehmen. Das Produkt arbeitet wie folgt: Das Mehrfach-Scanning erhöht die Erkennungsrate sowie den Schutz vor Malware, während das Abschotten der AV-Software diese sowie E-Mail-Server und Betriebssysteme vor Angriffen von außen effektiv schützt. Zum Einsatz kommt dabei eine 3-Tier-Hochsicherheitsarchitektur, die mit ihren Kontroll-, Abschottungs- und Vernichtungsmechanismen einem BSL-Klasse-4-Virenlabor (Biosafety Level) nachempfunden wurde.

Die Lösung wurde speziell auf die Sicherheitsbedürfnisse von großen Unternehmen und regierungsnahen Organisationen zugeschnitten. Darüber hinaus ist sie für alle Betriebe mit hohen Sicherheitsanforderungen interessant und zusätzlich durch die Zentralisierung des AV-Scannings ergeben sich Vorteile wie Hochverfügbarkeit und Ausfallsicherheit sowie Ressourcen- und Kosteneinsparungen.

Die Features von aps-AV in der Übersicht:

- **Schutz vor bekannten und unbekanntem Angriffen auf AV-Systeme**
aps-AV schützt Unternehmen vor bekannten und unbekanntem Angriffen gegen Anti-Virus-Engines. Durch die Installation auf dem E-Mail-Gateway werden auch die internen Clients und Server vor Angriffen auf die Anti-Virus-Engines geschützt.
- **Mehrfach-Scanning mit unlimitierter Anzahl von Engines**
Durch den gleichzeitigen Einsatz einer theoretisch unbegrenzten Anzahl von Anti-Virus-Engines steigert aps-AV die Erkennungsrate und bietet so maximalen Schutz vor neuen Gefahren bei geringen Reaktionszeiten.
- **Zentralisierung und Kostenersparnis**
Die aps-AV-Systemlösung mit allen eingebetteten Anti-Virus-Engines kann von einem zentralen Management-PC überwacht und konfiguriert werden.
- **Modular und zukunftssicher**
Die aps-AV-Lösung skaliert und wächst mit den Bedürfnissen der Anwender, ohne große Investitionen vornehmen zu müssen.
- **Sicherheits-Zertifizierung**
Die Zertifizierung von aps-AV nach Common Criteria EAL4+ und durch das BSI wird derzeit durchgeführt. Die Sicherheitstests selbst erfolgen nach EAL6.

Weitere Informationen finden Sie unter: <http://www.nruns.com/aps/presse.php>

Kurzporträt n.runs AG:

Die n.runs AG wurde 2001 mit Sitz in Oberursel gegründet und hat sich als herstellerunabhängiges und neutrales Beratungsunternehmen in den Bereichen IT-Sicherheit, IT-Infrastruktur und IT-Business sowie als Lösungsentwickler im Markt etabliert. Die Dienstleistungen des Anbieters verfolgen einen ganzheitlichen Ansatz und umfassen Audit/Assessment, Design, Unterstützung beim Einsatz neuester Technologien, Prozessberatung sowie Wissenstransfer. Gewachsen als Consulting-Spezialist, wurde das ursprüngliche Kerngeschäft später um die Sparte „Applications“ mit eigener Lösungsentwicklung erweitert. Im Zuge dessen hat das Unternehmen mit „Application Protection System – Anti-Virus (aps-AV)“ eine Hochsicherheitslösung konzipiert und entwickelt. Diese eignet sich speziell für die Absicherung und Zentralisierung von Antivirus-Infrastrukturen. Der Kundenstamm von n.runs besteht aus mittelständischen und großen Unternehmen unterschiedlicher Branchen wie beispielsweise Microsoft, Ferrero, 1&1, Deutsche Telekom und Daimler Chrysler.

<http://www.nruns.com/aps/presse.php>

Weitere Informationen:

n.runs AG
Nassauer Straße 60
D-61440 Oberursel

Ansprechpartner:

Torsten Pressel
Tel.: +49 (0) 6171/699-0
Fax: +49 (0) 6171/699-199
torsten.pressel@nruns.de
<http://www.nruns.com>

PR-Ansprechpartner:

Sprengel & Partner GmbH
Ulrike Peter
Tel.: +49 (0)26 61-91 26 0-0
Fax: +49 (0)26 61-91 26 0-29
E-Mail: presse@nruns.com