Virus scanners clear attackers a path into the network

n.runs warns:

Anti-virus software – from sentinel to spy

Oberursel, 27 June 2008 – During the past few months, specialists from the n.runs AG, along with other security experts, have discovered approximately 800 vulnerabilties in anti-virus products. The conclusion: contrary to their actual function, the products open the door to attackers, enable them to penetrate company networks and infect them with destructive code. The positioning of anti-virus software in central areas of the company now poses an accordingly high security risk. The n.runs AG is responding to this circumstance with its own system, aps-AV – a solution which secures the entire e-mail and anti-virus infrastructure and prevents such attacks.

The tests performed by the consulting company and solutions developer n.runs have indicated that every virus scanner currently on the market immediately revealed up to several highly critical vulnerabilities. These then pave the way for Denial of Service (DoS) attacks and enable the infiltration of destructive code – past the security solution into the network. With that, anti-virus solutions actually allow the very thing they should instead prevent.

In this context, n.runs was able to make out so-called "parsing" as one of the main causes of this boomerang effect. The principle functions as follows: virus scanners must recognise as many "Malware" applications as possible – and thereby comprehend and process a large number of file formats. In order to be able to interpret the formats, an application must partition the corresponding file into blocks and structures. This separation of data into analysable individual parts is called "parsing". Mistaken assumptions in the course of programming the parsing code create constellations which enable the infiltration and subsequent running of programme code. Moreover, the quick reactions time expected by developers (regarding threats) contributes to a decrease in the quality of the code. In short: the more parsing that takes place, the higher the recognition rate and the degree of protection from destructive software, but at the same time, the larger the attack surface – which makes the anti-virus solution itself a target. Systematic industrial

Presseinformation

and industrial espionage – along with the interruption of all e-mail communication – are merely tow of the possible consequences.

A shield for the anti-virus solution

To ensure that the virus scanner does not become a gateway to your network – and that attackers cannot assume control over it - n.runs has developed and launched the Application Protection System Anti-Virus (aps-AV). This solution, based on our own concept and development, completes companies' IT security infrastructure. The product works as follows: the multiple engines increase the detection rate and the protection against "Malware", while the firewalling of the AV software also protects e-mail servers and operating systems against attacks from the outside. In this process, a three-tier high-security architecture –follows the design paradigms of a BSL-4 virus laboratory, whereby control, shielding and destruction mechanisms are recreated.

The solution was custom-developed to meet the security requirements of large companies and organisations with government ties. In addition, it is of interest to all companies with high-level security requirements; it also offers advantages such as a high level of availability and system stability, along with a savings of resources and costs as a result of the centralisation of the AV scanning.

An overview of the features of aps-AV:

- Protection against known and unknown attacks on AV systems

  aps-AV protects companies from known and unknown attacks on anti-virus engines. The installation on the e-mail gateway also enables the protection of the internal clients and servers against attacks on the anti-virus engines.
- Multiple scanning with an unlimited number of engines

  Through the simultaneous use of a theoretically unlimited number of anti-virus engines, aps-AV increases the detection rate, which offers maximum protection from new dangers, with low reaction times.
- Centralisation and cost savings

  The aps-AV system solution, with all embedded anti-virus engines, can be monitored and configured from a central management PC.
- Modular and future-proof

  The aps-AV solution scales, and also grows with the company, without the necessity of large-scale investments.
- Security certification

  The certification of aps-AV according to Common Criteria EAL4+ (and by the BSI) is currently in progress. The security tests themselves take place according to EAL6.

You can find further information at: http://www.nruns.com/aps/presse.php

Presseinformation

Summary profile of n.runs AG:

The n.runs AG was founded in 2001 with its headquarters in Oberursel, and has established itself on the market as a developer-independent and neutral consulting company for the sectors of IT security, IT infrastructure and IT-Business, as well as in its capacity as a solutions developer. The services provided by this vendor pursue a comprehensive approach and encompass auditing/assessment, design, support in the application of the latest technologies, along with process consulting and knowledge transfer. Originally established as a consulting specialist, the company's original core business was later expanded to include the branch "Applications", with its own solutions development. In this process, the company has designed and developed a maximum-security solution with its "Application Protection System – Anti-Virus (aps-AV)". This product is especially suited to the securing and centralisation of anti-virus infrastructures. The n.runs customer base consists of mid-sized and large companies from various sectors – such as i.e., Microsoft, Ferrero, 1&1, Deutsche Telekom and Daimler Chrysler.
http://www.nruns.com/aps/presse.php

Further information:
n.runs AG
Nassauer Straße 60
D-61440 Oberursel

Contact person:
Andreas Tewes
Tel.: +49 (0) 6171/699-0
Fax: +49 (0) 6171/699-199
andreas.tewes@nruns.de
http://www.nruns.com

PR contact person:
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

Presseinformation