n.runs AG
Nassauer Straße 60
D-61440 Oberursel
Phone: +49 (0) 6171/699-0
Fax: +49 (0) 6171/699-199

n.runs aps-AV® - The next generation of AV-Security

Centralization and Multi-Engine Protection against new Email and AV attacks

aps-AV is a flexible and scalable high-security solution that has the ability to offer scanning and protection through the use of an unlimited number of AV engines. The result is a higher level of protection combined with potential savings and the protection of resources.

n.runs aps-AV® (Application Protection System Anti-Virus) is part of the n.runs aps product line. aps-AV offers comprehensive protection by implementing the Defense-In-Depth-Principle in a high-secure 3-Tier architecture. aps-AV not only offers multi-engine protection and the possibility of centralization but encloses the AV engines within a sealed environment. Furthermore aps-AV optimizes the performance of the servers and simplifies the administration of multiple AV engines and resources.

Even today classical malware attacks spread via email can still be considered a resource and cost-intensive threat to companies. In addition to these classical malware attacks, a new kind of attack targeting the AV solutions themselves has emerged.

These new attacks may have the following impacts :

- Wherever data is examined by AV software exploit code can be triggered. This can result in an attacker possibly being able to read complete email exchange and to execute further attacks in internal network segments. This may happen even when AV scanning and email servers are separated from each other.
- A denial-of-service attack against the AV solution (i.e. in the event of an attack that is not cleanly executed) This could mean the outage of the complete email infrastructure.
- Viruses and other malware can be delivered to the end user by completely bypassing the protection of the AV solution.

Where do these new attacks come from ?

The parsing engine is an essential component of every AV engine. In order to make binary data interpretable and comprehensible, they are split into blocks and structures. This process is known as “parsing“. Through false assumptions during parsing, conditions occur which allow program code to be infiltrated and executed. The SANS Institute included AV software as one of its Top-20 security risks[1].

Why are the consequences so huge?

One of the reasons can be seen in the attempt to protect all business relevant servers and clients of the company through software that is run with the highest privileges. Many times several AV engines are being used which drastically increases the attack surface and increases the chances for a successful attack.

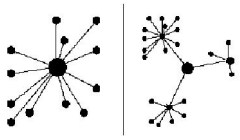
What kind of damage can be caused ?

- **External Costs:** claim for indemnification, higher interest rates for loans/ credits (Basel II, Solvency II) and penalties
- **Internal costs:** loss of intellectual property (75% of business information is being exchanged via email), labor costs during system and operating standstill after an outage, loss of sales through a lack of operational ability, the overloading of IT administration and Helpdesk resources
- **Indirect consequences** in case of non-observance (§ 91 AktG, § 93 AktG, § 276 Abs. 2 HGB, risk of liability or inprisonment in case of incorrect or non-existing accounting) resulting from incorrect data handling, data loss or manipulation through AV attacks: compromise of the existence of companies, loss of credibility and reliability, loss of image and market shares

A 2,000 person national law firm CIO estimates a recent **email outage** cost the firm $100,000/hr in lost revenue and productivity.

Source: MessageOne

What does Centralization mean ?



Centralization in the context of aps-AV means that data is not checked locally but centrally in a protected aps-AV environment. Centralisation and localisation can coexist as shown in the illustration on the right.

Advantages of the AV centralization

Centralization can lower AV license fees and preserve personnel resources as the installation and management of several AV products increases the administrative overhead. Furthermore aps-AV is able to receive other data, besides email, and can therefore be connected to SAN, file servers, web servers and many others, furthermore aps-AV does not have a single point of failure.

aps-AV is modular and future proof

aps-AV scales and grows with the requirements of your company and does not cause major restructuring or expenditure of time.

[1] http://www.sans.org/top20/#s5

What are the features of aps-AV ?

Security and Protection

- **Zero-Day Protection**

aps-AV protects your company from known and unknown attacks against Anti-Virus engines and further protects all internal Anti-Virus Systems and E-mail servers from remote zero-day attacks. The existing internal AV clients and internal email servers are protected against any attacks by embedding aps-AV into your email gateway or, alternatively, your server.

- **Failsafe Protection**

aps-AV manages engines in such a way that it can guarantee that if one engine fails to update or to start, the other engines continue to protect your environment with no delay. Additionally our Q&A department verifies the updates manually in order to allow for a highest possible level of assurance.

- **Multi-Engine Protection**

Through the simultaneous use of a, theoretically, unlimited number of AV-engines aps-AV increases the overall detection rate and is able to offer the highest degree of protection against new threats with the lowest possible reaction times. aps-AV automatically downloads the latest signatures ensuring a high level of protection, and reduces the window of exposure to any given threat.

- **Roll-Back Support**

In the event of an flawed Vendor update, aps-AV offers a Roll-Back function. As such aps-AV can rollback to the latest stable version of the AV-engine within seconds. Through this feature the protection is guaranteed for the time that the AV vendor requires to fix the problem. The same feature allows AV engines to be exchanged during operations without any delay or interruption of E-Mail service.

- **Qualiy Control of AV-Updates**

Updates from AV vendors are subject to a manual quality assurance process, this guarantees the highest level of stability. Depending on the assurance level that our client requests, our support and Q&A Department is performing Q&A checks of the engines and only after successfully passing the Q&A cycle they will be signed and sent to the client where they will automatically be integrated.

- **Protects Your Most Valuable Assets**

aps-AV can be configured to offer advanced protection to highly sensitive recipients such as board of directors and employees in research or accounting, this leads to lower costs, since in total, less licenses may be required.

- **Protection Against Unknown Threats**

aps-AV includes heuristics that detect malicious code based on behavioral analysis. Through the usage of diverse engines and diverse heuristics detection is further maximised.

- **Reduces the Time Window to a Minimum**

The critical time window between the discovery of a new threat and the update of a signature to detect the threat leaves companies vulnerable to attack. With aps-AV, multiple vendors are acting upon a new threat at the same time, increasing the chances for fast detection and lowering the business risk

- **Security-Certification (EAL4+)**

EAL4+ certifications is currently ongoing. Security Tests are being performed according to EAL6.

- **Highly Secure Communication Protocol**

The different systems can only communicate across the security layers by means of a special multi path protocol developed in accordance with the security requirements of the architecture. Only strong and proven crypto algorithms are being used, with no trust relationships and every communication is authenticated anew.

Performance

- **Zero Downtime**

aps-AV is able to continue scanning e-mail with all engines, even while engine or signature updates are ongoing. Updating engines is a matter of seconds while the other engines continue scanning for Viruses. The result is no delay and continuous mail flow.

- **Full Redundant Architecture**

Optionally, the aps-AV architecture is designed to be completely redundant. This ensures that the AV protection is not influenced during outages or during the maintenance of hardware components.

- **Optimized Performance through Caching**

aps-AV uses a cache preventing the useless multi-processing of data; i.e. when sending emails to multiple recipients or sending to mailing lists. This feature increases the performance of the system, preserves resources and speeds up email delivery.

- **Mail Cluster support**

aps-AV can be custom tailored to your requirements, due to the three tier architecture it is by it's very nature modular and adaptable to your needs. Supports e-mail architecture (Exchange, Notes, Qmail, Postfix etc.)

Simplefied management

- **One-Stop Automated Updates**

AV Updates are delivered with no stress on internal IT resources. Once the updates have passed the Q&A cycle n.runs keeps all of the engines and signatures up-to-date automatically. Furthermore the updates are digitally signed to ensure traceability.

- **1st through 3rd Level Support**

n.runs AG offers direct and qualified 1st level support 24x7x365 and direct 2nd through 3rd level support.

- **Protection of Investment**

The modular and flexible architecture supports any email architecture; if desired even self-developed or specialized architectures. Therefore email migration is not a problem at all. Furthermore any AV engine can be integrated. This reduces the effort of AV migration to a simple configuration task that can be done by a few mouse clicks.

- **No Expensive or Special Hardware**

The aps-AV system solution does not need any special or specially certified server hardware. Hence the costs for the stocking of replacement hardware are low.

- **Modular and Future-Proof**

aps-AV scales and grows with your company protecting your investments, the Front Tier (IOFE) can be transformed into accepting data other than mail through the open interface of the IO front ends.

Centralization

- **Cost Savings and More**

The centralization aspect of aps-AV allows centralized multi-scanning, TCO reduction through a decrease of hardware costs (decrease of power, space of the data processing center, cooling) and the possibility to support legacy systems that are not supported by AV producers (anylonger).

- **Standardized AV-Policy**

aps-AV offers a standardized AV policy for heterogeneous environments and the possibility of group policies for AV scanning (i.e. 5 AV engines group 1, 2 AV engines group 2).

- **Centralized Management**

aps-AV and all AV Engines can be managed and configured by a central management PC. This allows for no additional administrative overhead due to the increased number of AV Engines.

n.runs AG
Nassauer Straße 60
D-61440 Oberursel
Phone: +49 (0) 6171/699-0
Fax: +49 (0) 6171/699-199

More information about aps-AV can be found under **www.nruns.com/_en/aps**