



Insurance against unwelcome occurrences in IT security

SecuLution ensures unhindered access for high security.

"As a university teaching hospital, we must take into account the users' wish for unhindered Internet access. After all, scientific work includes global research, study comparisons and communication with colleagues. On the other hand, there are constantly new mechanisms that can harm the company in the World Wide Web." This is how Ralf Plomann, IT manager at St. Marien's Hospital, Lunen describes the predicament in which he finds himself. He often feels as if he is the hare racing against the tortoise and that he cannot really win. "The software manufacturer's security patches are often not available quickly enough, and we are unable to test them during the work day for compatibility with existing solutions." Firewalls will only provide support security, anti-virus programs respond only to known viruses and trojans.

So what to do to guard against security gaps, and to allow employees to have safe and easy access to the web? "We looked around for a solution that prevents employees from executing programs that were not approved by IT," Plomann explained his approach. With this in mind, the St. Marien's Hospital discovered SecuLution and quickly realized that the software will help to solve many problems. Now, about 650 computers are protected in both of the St. Rochus GmbH's buildings - and this will continue to increase. In 2011, this solution will be used in the entire clinic.

Simple configuration of a whitelist

"Due to the performance of the product, I can calmly face many

problems, while colleagues in other clinics are very concerned," says the IT manager. The IT Security Suite SecuLution technically ensures that only software that is classified as trustworthy on a central Positive List, the so-called whitelist, can be executed. In other words, that means: any software that is not recognized will not be executed. That lets computers be what they are: work tools with only the software that is required for work. And the security is above and beyond the PC itself. USB devices and all removable storage devices can be managed in the same way. The same rules apply here: if it is neither recognized nor allowed, then it cannot be used. "Many think that an enormous amount of work is required to create a whitelist. That would be the case if SecuLution did not install clever mechanisms that make the entire effort very manageable. That is exact-

ly the main attraction of this security solution,” said Plomann enthusiastically. It would require a lot of effort to manually enable the complete whitelist with thousands of files per computer. That is why SecuLution offers a “Learning Mode” with the first configuration. “Additionally, we have selected a safe and clean computer that has updated software and access to the internet and USB devices. This sample computer’s complete configuration was imported into the positive list,” Plomann described the procedure.

The learning mode was then centrally activated, and the SecuLution Agent was rolled out on all network computers by the built-in Agent software deployment. Now the users have been working as usual for a month with their programs. So any additional software that does not exist on the sample computer is detected and automatically transferred to the central approval configuration. During the learning phase, the user did not face any restrictions. At the end of the month, the system administrator looks at the list of programs added during the learn phase and can remove any unwanted or non-relevant work programs. The administrator received a surprise when he saw all of the non-relevant software that the users have on their computers.

SecuLution honours promises

“We were particularly impressed with the extremely high functionality of SecuLution. For example, some versions of executable files could be blocked but similar programs were not able to do this. Additionally, SecuLution is a privately owned medium sized company with lots of know-how and great customer service. This was seen in intensive personal conversations and presentations,” Plomann explained the reasons for the collaboration. Last but not least the convincing price performance ratio significantly supported the decision. Thus, even the hospital’s affiliated Nursing School with a modest IT Budget could use the solution.

Nevertheless, before the introduction, the IT manager was very sceptical of the security and administrative investment. “We first had to convince the users and administrators of the usefulness of the project and the solution. The aim was primarily to remove the fear of additional work load and to communicate the benefits of the solution in the daily routine,” said the IT Manager. That’s why the project started with a small installation. SecuLution was quite convincing and it rolled out in stages. “Currently the solution is enjoying a very high acceptance level and all administrators are satisfied.”

Simple configuration and quick rollout

How exactly does SecuLution actually work? At the end of the learning phase, the system had an inventory of all software that is used in the network. This status quo can be edited by the administrator or simply be “frozen”. SecuLution is a Client-Server System. The system servers are connected to the network and the client installed on each host to be protected. It can be determined centrally for all systems on the server which programs are allowed to be used.

Every attack on a network requires that a program run on a computer. SecuLution identifies each program to be executed on the host, on the basis of an elec-

St. Marien’s Hospital, Lünen

The St. Marien’s Hospital has 590 beds and is one of the largest Catholic hospitals in the Ruhr region and Münsterland. With a total of 16 departments, the focus of the hospital is maximum care of 20,000 inpatients and nearly 40,000 outpatients annually. The Academic Teaching Hospital of the Westfälische Wilhelms-Universität Münster together with the St. Christophorus’s Hospital Werne (216 beds, 9,000 inpatients and 12,000 outpatients per year) forms the hospital group St. Roch GmbH.

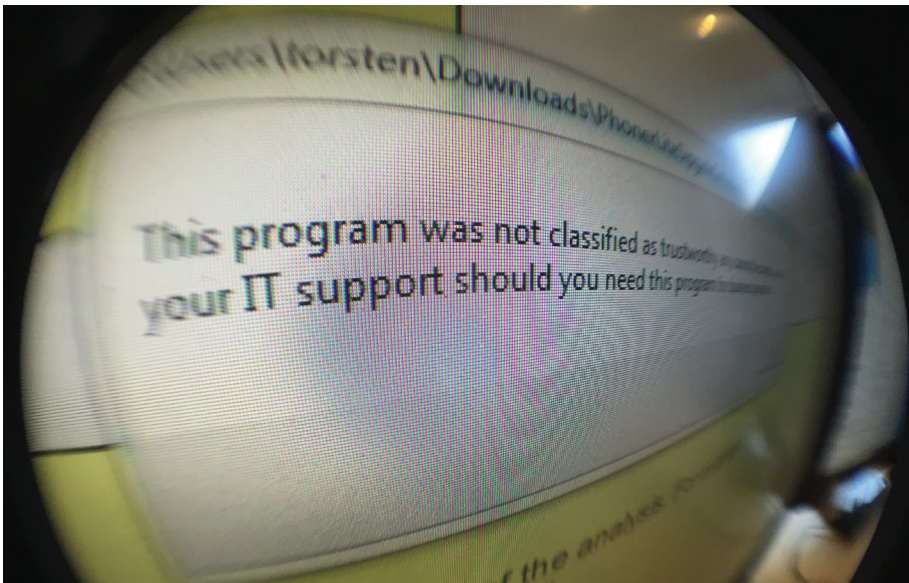
SecuLution

SecuLution is the leading provider of proactive security solutions for enterprise networks. The self-developed and internationally patented SecuLution solution protects networks in a revolutionary new way against all types of attacks. In addition to security training and consulting services, SecuLution also issues recognized expert analysis of existing network and security structures or analyses and documents attacks. The core of the corporate philosophy is the safety and satisfaction of the customers. The staff are consistent and competent in the design and implementation of security without losing sight of operating efficiency. Security is seen as a means to increase the productivity of systems while reducing operating costs. Both the products and services are based on this.

tronic fingerprint - immediately before the execution. Using the administrative console called “Admin Wizard”, the administrator can centrally set which programs on which computer are allowed to be started and by whom. If a user attempts to execute an unauthorized program, an alarm is triggered in SecuLution before it is executed and the program is blocked. “We can



Ralf Plomann, IT Manager Hospital Group
St. Rochus GmbH



SecuLution ensures unhindered access for high security.

without any extra effort: It is sufficient when the administrator completes the installation on any computer using a user account that was previously defined as a permanent learn user. The new software can be installed without further modifications on all other computers in the network. Windows updates are automatically integrated so that manual interaction is not necessary. During normal operation, no additional administration costs arise.

High Security at Low Cost

"In my eyes SecuLution is the sedative for administrators. I'm really happy to be working with the system. It saves me a lot of effort and gives me time for other activities," the IT manager Plomann brings his experiences of the past five years to the point. Since the user in the clinic cannot slow down their systems by starting unwanted software, the first- and second-level user support has dropped considerably.

The systems are stable over time, which has had a positive effect on administration costs as well as higher productivity. In addition, the cost of safety administration dropped significantly. It eliminates any search for successful attacks or virus attacks, it is not necessary to do audits of network traffic or log files from IDS logs.

"And even if the servers fail, SecuLution continues working safely because authorized programs are cached locally on

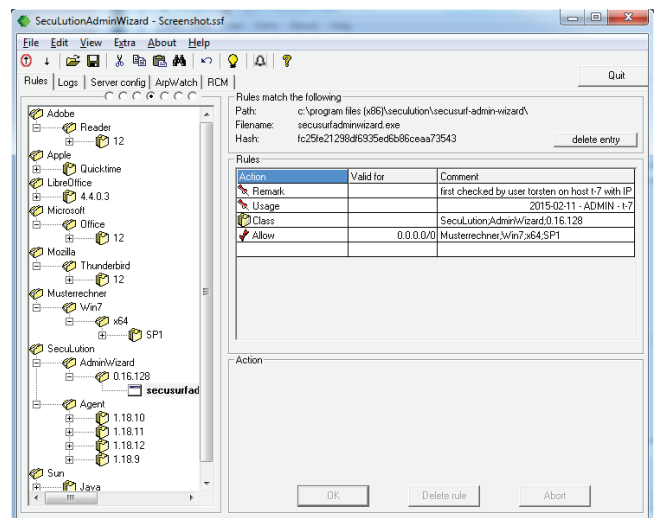
each PC so that even mobile devices that do not have constant connection to the internal network can be secured," adds Plomann.

Finally, the software supports the IT department in consolidation of the application environment. Based on dedicated evaluations, it can quickly be determined which programs are no

longer needed and can be deleted from the servers. The value of the investment for security software in IT is measured by the number of

individually specify how a computer should behave when an unwanted action is performed on it," explained Plomann. "Generally, the execution of the program is blocked, a warning pops-up and the user is referred to IT Support. Other actions are possible such as a forced immediate shutdown of the computer." An extraordinarily high level of safety is ensured as it is technically not possible to have unauthorized programs.

If a user requests an application that he would like to use, adding it to the whitelist as well as the authorization is completed with a mouse click in the central management console. The user can immediately use it without delay. The administrator has many possibilities to adapt the rules. The installation of new software as well as the updating of existing software requires changes in the checksum and calls for an adaption of the standard rules. This is completed



With little effort, new applications can be locked or unlocked.

unpleasant incidents not occurred - and we've never had one," concluded Plomann.

Provider

SecuLution GmbH
Alter Hellweg 6 b
59457 Werl
Germany
Tel.: +49 2922 9589210
E-Mail: info@4ss.de
http://www.4ss.de

Case study reference

Krankenhausverbund St. Rochus GmbH
Ralf Plomann
IT-Manager
Altstadtstraße 23
44534 Lünen, Germany
Tel.: +492306 772170
E-Mail: plomann.ralf@klinikum-luenen.de