

# Virus Protection at the University Hospital Basel, Switzerland

The University Hospital in Basel provides a good example of broad-based virus protection for medical technology systems. With Siemens Virus Protection, the hospital proactively protects most Siemens modalities against potential attacks.



“Today our capacity is configured in such a way that the devices always have to be functioning. That’s why in addition to system quality, operational security is our most important goal.”

Professor Wolfgang Steinbrich,  
Director of the Institute for Diagnostic Radiology,  
University Hospital Basel, Switzerland

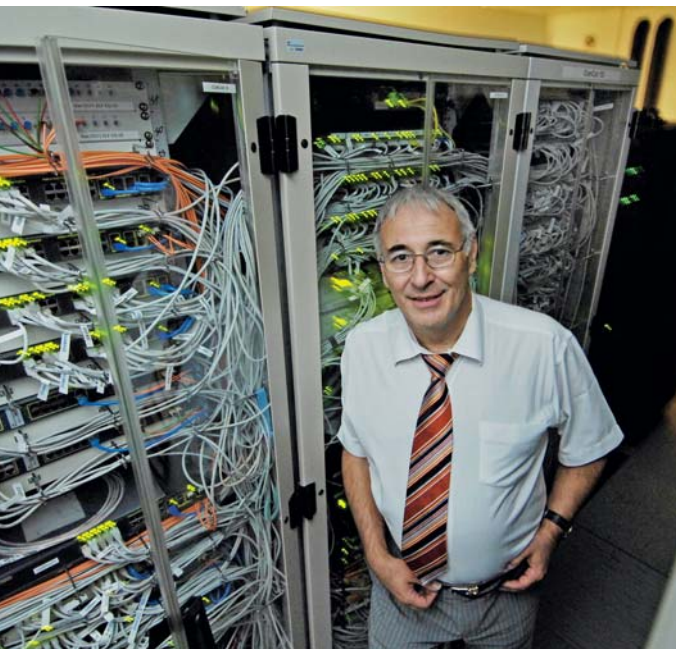


In the University Hospital Basel, on a daily basis, about ten thousand patient images – corresponding to a volume of 18 gigabytes – are processed and registered in the network of the radiological image storage system. Currently, the entire quantity of stored image data amounts to about 32 terabytes, which is equivalent to the contents of over 5,000 kilometers of file shelves.

## Providing operating security for the systems

Given the high level of system utilization, equipment reliability is crucial. And security considerations play an increasingly important role in providing this reliability. On the one hand, networked communications and the exchange of data worldwide brings the risk of contamination by malicious software, such as viruses, worms, and Trojan horses. On the other hand, the systems need to be protected from risks resulting from

the hospital’s internal operating network. The systems are increasingly threatened by viruses stemming from data exchange, for example through USB devices and network-connected laptops or from files downloaded from the Internet. For the University Hospital Basel, the safety and protection of medical technical systems with their enormous volumes of data have top priority. Professor Wolfgang Steinbrich, MD, Director of the Institute for Diagnostic Radiology, explains: “Today our capacity is configured in such a way that the de-



“If I open a network connection to the outside world for the protection of our own network, then it’s important for me to work together with an expert provider. With Siemens we can implement this innovative protection.”

Franz Buffon, Director of IT, University Hospital Basel, Switzerland

vices always have to be functioning. That’s why in addition to system quality, operational security is our most important goal.”

To achieve this, the University Hospital Basel installed full-scale protection against malicious attacks – the first hospital in Switzerland to take this step. To protect against viruses, worms, and Trojan horses, most imaging systems from Siemens are equipped with Siemens Virus Protection.

The University Hospital currently has 27 Siemens modalities that are secured

through Siemens Virus Protection. The service consists of virus detection and elimination as well as prevention. Through the installation of a virus scanner and connection of the systems to Siemens Remote Service (SRS), remote updates with relevant hotfixes are imported proactively to protect the systems against attacks from every type of known virus. Should a virus infection nevertheless occur, the Siemens experts can frequently detect this very early – thanks to remote monitoring via SRS – and take suitable action before the cus-

tomers are even aware of the virus on-site and before the virus can cause any damage. Professor Steinbrich values this aspect in particular: “It’s our responsibility to safeguard and protect our image data. Due to new technologies, new dangers have arisen that we must eliminate. I was very positively impressed by Siemens’ proactive approach with Virus Protection. That’s why I strongly supported this solution.”

The director of Medical and Operational Technology, Christian Kluth, attaches special importance to ensuring that all

Siemens Virus Protection continuously monitors the large-scale equipment operated at the University Hospital Basel. This includes systems used in various areas, such as angiography, computed tomography, magnetic resonance tomography, and medical imaging stations. The solution includes proactive virus protection as well as virus detection and virus elimination. Virus Protection is one of the innovative service offerings made possible by Siemens Remote Service (SRS), the infrastructure for long-distance data transmission.

### The benefits at a glance

- Reliable protection against software attacks
- Expert problem resolution
- Reduced technical and IT costs
- Smoothly running clinical routines
- Higher system availability
- Improved efficiency
- Increased planning security

“Just one insecure site would be one too many. Only the installation of Virus Protection in all equipment offers the protection we prefer to help ensure the operating reliability of our machines and systems.”

Christian Kluth, Director of Medical and Operational Technology,  
University Hospital Basel, Switzerland



large-scale equipment in the University Hospital Basel is equipped with virus protection. As he says, a complete solution of this kind is a highly feasible approach for providing comprehensive protection against virus attacks: “Just one insecure site would be one too many. Only the installation of Virus Protection in all equipment offers the protection that we prefer to help ensure the operating reliability of our machines and systems.”

Professor Steinbrich attributes the dangers to two principal causes: “First, clinical

diagnostic equipment has become highly developed – from the original precision mechanical systems with analog electronics to computer-controlled instruments with complex software for digital imaging. Second, the stand-alone workstation systems of former times are today interconnected and networked with the image viewing units of image storage networks. In addition, a high-performance link to the radiological information system and to the hospital-wide network of the clinical information system is planned.” Steinbrich con-

cludes: “Although the different networks are physically decoupled, they are connected through the exchange of information. In order to prevent the misuse of personal data at the interfaces and to avert threats, for example, from Trojan horses or viruses, comprehensive innovative protection systems are required – such as Siemens Virus Protection.”

### Contact

[birgit.munz@siemens.com](mailto:birgit.munz@siemens.com)  
[www.siemens.com/virus-protection](http://www.siemens.com/virus-protection)