VDGH
Verband der Diagnostica-Industrie

Positions of the VDGH working group “IT-security”

January 2020

IT Security of IVD Devices including Legacy systems in the hospital and laboratory environment

In vitro Diagnostic (IVD) devices have various applications in modern hospital and laboratories. From analyzing blood samples of patient concerning possible infections to the amplification of a targeted DNA molecule using polymerase chain reaction techniques, IVD devices are essential for modern medicine. To improve the utility for patient and physician, modern IVD devices are often connected to the hospital information system (HIS) or even the internet. While the increasing number of connections between various devices is mandatory to reach these goals, IT security of these devices has to be maintained under any circumstances.

This paper gives guidance which actions should be taken by the user in the hospital or laboratory environment to maintain safety and essential performance of IVD devices. These actions are depending on the current phase of the IVD device within its product life cycle. While the proposed actions include various forms of updates of the IVD device, the IT security of all relevant software systems in the hospital or laboratory should also be kept in mind. Consequently, the proposed actions are not only relevant for the IVD device itself but the overall IT network and all connected medical devices of the hospital.

These actions are in detail:

Functional Updates

Functional software updates are issued for all reasons concerning the function of the product by manufacturers of software solutions, ranging from the updates of established functions to the introduction of new features to increase the user experience. They also include patches to remove software bugs identified after release to maintaining the compatibility with other devices, software, and operating systems that interact with the IVD device.

The user should make routine system updates concerning functional updates part of best practice of a hospital or a laboratory. The latest updates ensure the optimal performance of the system and the compatibility with other devices.

IT-Security Updates

IT-Security patches are issued to fix software vulnerabilities that lead to possibilities for external forces to corrupt the function of the systems due e.g. ransomware, Malware and all kind of other computer viruses. IT-Security patches are issued by manufacturers as soon as possible after software vulnerabilities become known.

A management program focusing on secure importation and implementation of trusted patches will help keep control systems more secure. This includes cybersecurity updates and patches of the operating system, IVD devices (provided by the manufacturer), hospital information system and the relevant software on all connected IT systems.

The user should make routine system updates an integral part of the cybersecurity best practice of a hospital or laboratory. The latest updates for all connected IT systems should be installed.

Hardware Upgrades

Hardware updates include all parts of the hardware system that can be updated to increase its capacity to run the latest version of software (including operating system and third-party software). This includes new hard disks, new CPUs, RAM or the exchange of the mainboard of a system.

Services

Services of manufacturers included the maintenance, repair, delivery of exchange parts and telephone and e-mail support.

Categories of IVD devices based on the product life cycle

Defined by the phase of their product life cycle, IVD devices are supported differently by manufacturers. To improve the IT Security of the IVD device, corresponding actions for the user are displayed in the following.

1. Systems in production – full support by the IVD manufacturer

This category includes all systems that are still being manufactured and sold, and that are under full support by the manufacturer. To maintain the necessary level of IT Security the system should receive the latest:

- Functional updates
- IT-Security updates
- Hardware upgrades
- Services

A replacement of the system is not necessary in the current phase of the product life cycle. The support of the system with IT Security updates is ensured by the IVD manufacturer for the foreseeable future.

2. Systems after end of production – full support by the IVD manufacturer

This category includes systems that are not manufactured and sold anymore, but that are under full support by the manufacturer for an extended but clearly limited time period. To maintain the necessary level of IT Security the system should receive the latest:

- Functional updates
- IT-Security updates

- Hardware upgrades
- Services

A replacement of the system is not necessary in the current phase of the product life cycle. The support of the system with IT-Security updates is ensured by the IVD manufacturer. However, due to the expected end of the support by the manufacturer, the replacement of the system should be planed for the near future.

3. Systems after end of production with limited support by the IVD manufacturer

This category includes systems that are not manufactured and sold anymore; with a short remaining time period of limited support by the producer with:

- IT-Security updates
- Services

The support of the system with limited IT-Security measurements is ensured by the manufacturer for a limited time period. A replacement of the system will be necessary in the near future.

4. Systems after end of product life cycle without support by the IVD manufacturer

This category includes systems that have reached the end of their product life cycle. The manufacturer does not offer any IT-Support including software and cybersecurity routine updates for the system.

The immediate replacement of the system is recommended to ensure the IT Security of system.