Remote Access for Remote Services (RARS) Scheme

In an ever-changing world, where mobile applications are becoming more common, cybersafety and cybersecurity become more and more an issue. How can you assure your customers your remotely accessible system is free from security flaws that could be abused by adversaries to hack into your system and worse: get access to sensitive information?

Kiwa can help you. By taking the recent cybersecurity trends into account, Kiwa developed the Remote Access for Remote Services (RARS) scheme. The RARS scheme is a collection of assessments set up by Kiwa that focuses on different kinds of systems that are remotely accesible. An alarm system which can be operated with a mobile application is a clear example of such a product. Remotely accessible systems are made up of an enabling chain of entities which have to be addressed individually as well as integrally. Together we can create trust in the whole chain of your product and make sure it is safe and secure.

Remote Access

Remote access: the ability to access a network or computer from afar through the use of a network connection. This enables users to access the systems at any given time. In this way it is possible to remotely perform certain actions and operations on systems. Remote access of systems is made possible by the rapid sophistication of hardware and software in the end creating very complex and multi-layered systems. This naturally means that the security risk becomes higher because the products are made up of several components and have multiple factors that influence its overall safety.
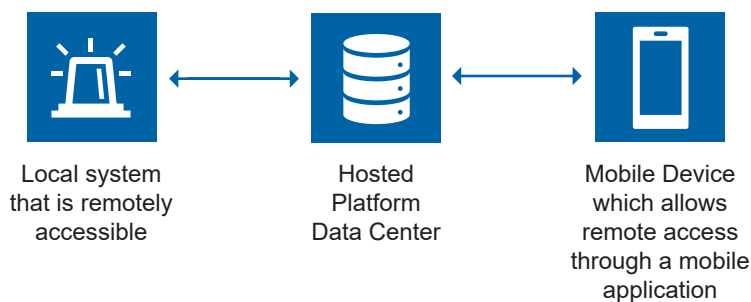
The RARS scheme offers a solution to the previously mentioned risks and forms a foundation of security whereupon you can build. By combining multiple areas of expertise within one scheme safety and security can be assessed integrally.

How does that work for your systems?

All data, that comes to or goes from a system, must undergo various processes. Every process is related to a specific part of the system. A system, roughly speaking, consists of three main parts: a Data Center, some kind device that allows remote access through the means of a mobile application or something as a panel and a local system that can be accessed remotely, as can be seen in the diagram below.

Local system that is remotely accessible

Hosted Platform Data Center

Mobile Device which allows remote access through a mobile application

Explanation of the diagram:

The local system is a combination of physical equipment and the software running on the device. Both are collaborating with the ultimate goal to fulfill the functionality of the system in case. The data generated in the local system is routed to the online hosted platform, The Data Center (DC).

The Data Center (DC) is a hosted platform and can be seen as the linking pin of the entire system. It represents the operations and interactions of the data, that is generated in the local system itself. All with the purpose of forwarding the information to a device that allows remote access: for example the mobile phone of a user (e.g. mobile devices and web apps).

The mobile device represents the group of devices that are utilized for remotely accessing the functionality of the local system and is connected to the hosted platform / data center. After the data is processed by the DC, the application of a mobile device can be used to remotely operate and monitor the alarm system.

Why RARS?

When your remotely accessible product is in compliance with the RARS scheme you as a manufacturer, producer or supplier can show that your product is actually safe and secure. With the corresponding certificate you can assure your customers that your product including mobile application is safe and secure.