advenica

SOLUTION DESCRIPTION

Secure Remote Access

Many organisations depend on remote access through RDP, for example to allow suppliers to perform maintenance, or so that operating personnel can monitor and control a system. Secure remote access solves many of the security risks that are otherwise associated with such solutions.

Challenge

Create Secure Remote Access

It is very important to be able to manage and monitor systems remotely. General network connections such as IP-Sec or TLS are sometimes used to connect data networks remotely. In terms of IT security, such connections mean that both systems are exposed to the sum of the threats facing each of them. A common feature of many remote access systems is that they are universal and have adaptations and functions for everything from office work to system administration. This also means that there are risks of both incorrect configuration and implementation bugs.

In addition to bridging geographical distance, remote access systems are often used increasingly to enhance security. A jump server is often used as an intermediary. The aim is to limit any undesired traffic from the user's PC to the target system. The software that the user wants to use is run on the jump server and communicates with the target system via standard protocols. These are some of the risks of such solutions:

1. The risk of unauthorised persons using the connection

Most systems have functions for authenticating users so that unauthorised persons cannot use the connection. However, sometimes the focus is more on ease of use or performance than on security.

2. The risk of the connection being used at the wrong time

When suppliers need to access the system, there is a risk of them misusing their authority at times other than the agreed time. This may not necessarily be intentional. It may equally well be that the supplier's IT system is exposed to an attack, which leads to a follow-up attack.

3. The risk of the connection being used for the wrong purpose

It is very common for the connection to have more extensive authority than is needed to perform the task at hand. The risk is then that the user can make intentional or unintentional mistakes. It also means that you can be exposed to the risk of a follow-up attack if the user's system is attacked.

4. The risk of connecting peripheral devices

Several of the protocols have functions for connecting peripheral devices. These may be speakers and microphones, printers or removable media such as USB sticks or hard drives. It is sometimes possible to switch off these functions in the configuration. However, you need to be sure that this has been implemented securely, which is not always the case.

Solution

Secure and Easy to Use

Remote access can be made secure by using RDP and protecting the jump server with an explicit security solution. SecuriCDS ZoneGuard for RDP is such a solution. The connection from the user's PC is established with RDP to ZoneGuard. The user is authenticated and the solution ensures that the connection is to an approved target system at a permitted time. ZoneGuard then ensures that only screen view data may pass from the target system to the user. Only keystrokes and mouse movements are transferred in the other direction. It is also possible to set restrictions, for example that only certain keystroke combinations are permitted. No other information is permitted to pass, eliminating the risks of, for example, general network communication or incorrect configuration of the jump server or its software. This also prevents access to peripheral devices, which would otherwise have meant enhanced risk.

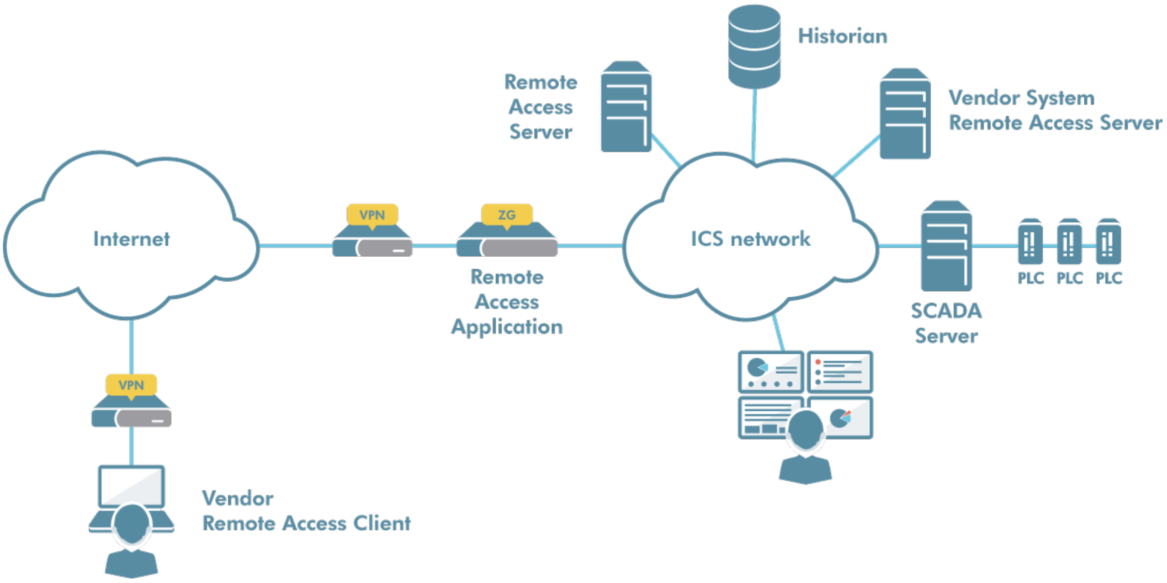
Advantages

Security and Functionality

Using RDP and protecting communication with ZoneGuard achieves both security and functionality:

- Only authorised users can use the connection at permitted times.
- The connection can only be made to the systems intended.
- No risk of transfer of malicious code at network level.
- No exposure to peripheral devices.
- Traceability: who did what when?

To read more about ZoneGuard, please visit advenica.com.


Historian
Remote Access Server
Vendor System Remote Access Server
Internet
VPN
ZG
Remote Access Application
ICS network
SCADA Server
PLC
PLC
PLC
VPN
Vendor Remote Access Client

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read more at advenica.com

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED