THINK BIG. GO BEYOND.

Cyber Security for SCADA Systems

Today's SCADA systems are more interconnected than ever before. The internet of things has allowed all types of automation systems to achieve efficiency and control that would have never been possible just a few years ago. This trend has caused systems to become merged with and dependent on IT infrastructure. While servers, network-based controls, and remote access to systems provide great value in a SCADA system, they also introduce security concerns that must be considered.

QUESTIONS TO ASK YOURSELF:

Do critical PCs and servers have access to the internet?

How are you accessing the system remotely?

Do vendors have remote access to your system?

Are you utilizing cloud services to host data or applications?

Is your firewall configured properly?

Are servers & PCs patched regularly?

Are functional system backups available?

FOR MORE INFORMATION:
Jason Schuler
Security Specialist
701-746-8087
Jason.Schuler@ae2s.com

CYBER SECURITY "TOP TIPS"

Allow access to the internet only where necessary. Use PC on separate network if full internet access is required.

If integration between SCADA and enterprise network is required, use a firewall to limit access to SCADA.

Enforce minimum password length and use two-factor authentication, especially with cloud based services.

Establish monitoring systems to alert ASAP if issues arise.

Backup systems and periodically ensure functionality.

Give users access only to necessary services and do not share logins.

Patch PC and server operating systems and applications regularly.

If vendors require access, ensure access is only to necessary areas.

Use encrypted communications anywhere possible. For example, some older radio systems have encryption disabled by default.

Understand how to operate your utility manually if SCADA is compromised from a threat or natural disaster.