Royalty-free stock vector ID: 1462012349

Jun 08, 2020 16:53 BST

'30 minutes' webinar series: Top security issues facing industrial control systems (ICS)

It's a well-known fact across all industries that an organisation can appear to have all the controls and processes in place for resilience, but one weak spot can potentially threaten everything they've built.

In the context of industrial control systems (ICS), ensuring security gaps are bridged is essential for many sectors, including energy, production and transport.

This becomes even more crucial as operational technology (OT) interconnects with IT, and as Industry 4.0, connected cities and cloud services gain more and more traction – all of which open up a multitude of new risks and attack vectors.

Top security issues

Over the years, we've learnt a lot about the security issues that ICS are facing. As part of our 30 minutes webinar series, we wanted to highlight what these are, and what organisations can do to step up their security. Below are just five of the ten issues covered– if you'd like to find out more, watch the full webinar below.

1. Hardware and software visibility

Organisations often have a low degree of visibility and management of their asset landscape, which can lead to a range of security issues and weaknesses.

To help gain better visibility and asset management in the OT environment, a number of specialised tools are required that can help organisations to have a continuous overview of assets, as well as detect rogue or modifications of assets – often an indication of malicious activities.

2. Network segregation

Another issue we've come across is the poor segregation of supervisory networks and corporate networks, whereby remote access tools are connected to the OT environment and firewalls between networks are poorly configured.

To reduce risks, OT assets should be separated into security zones with proper rules for how data flows between sources.

Performing periodical network protocol analysis and using firewalls between each zone can also alleviate risk, as well as threat modelling exercises which can be used to identify potential attack vectors and architectural weaknesses in networks.

3. Credentials and access

We all know that secure credentials are important, but this is one area that we've seen organisations fall down on. Through hardware reviews and scanning, we've seen default credentials in use, low usage of multi-factor authentication, trivial passwords, shared user accounts and non-encrypted passwords.

This is particularly problematic for supplier remote access, and has led to a number of ICS incidents – including brute force attacks, password spraying and more.

To establish tighter measures around credentials and who can access which networks and accounts, strong authentication and secure principles need to be implemented – not just for internal users, but also for suppliers developing software or hardware.

Least privilege principles can also help to ensure only those that need to access certain environments, networks or accounts have the ability to.

4. Monitoring

Being able to monitor activity across a network is another important means of protecting ICS.

From our experience, we've found that few organisations have insight into OT components and network activity, with very little real-time or even near real-time detection capabilities. Given this, there should be an expectation that someone already is, or will be testing the defences of your systems and networks.

To detect sooner and safeguard against potential attackers, employing real-time monitoring capabilities is advised, where possible. This can help to identify any unusual traffic on and between security zones, monitor access and/or changes to safety instrumented systems (SIS), as well as changes to field devices.

5. Awareness

While technical aspects of ICS security are important, raising awareness and sharing knowledge helps to bolster security posture on the frontline. It's well-known that a number of threats can be mitigated by doing this, particularly as phishing continues to be an effective attack method.

This is often down to a lack of collaboration between OT-security and IT-security, education, and discrepancies in jargon between OT-operational staff and IT-security staff.

To bridge this gap, training staff on the common threats that usually aim to exploit their human weaknesses can give you a base-level of defence. On top of this, sharing and implementing a common cyber security language can help align OT and IT teams.

Securing the future of ICS

As the Centre for Internet Security rightly puts it: "How can you protect yourself if you don't know what you have?"

Harnessing the power of OT and IT will be critical in the years to come, so it's important that organisations are able to identify any gaps in their systems, processes and education.

While a number of threats to ICS continue to prevail, if organisations consider the above and further measures set out in the webinar, they will prove to be in a much stronger position to tackle these and ensure that critical systems continue to run.

Watch the full webinar here.

View embedded content here

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970