

COMMENTARIES [\(https://www.americancityandcounty.com/programs/commentaries/\)](https://www.americancityandcounty.com/programs/commentaries/)



COMMENTARY

5 steps to reduce risk for critical infrastructure and industrial control systems

Written by Aleksander Gorkowienko 24th April 2019

(<https://www.americancityandcounty.com/files/2019/04/Aleksander-Gorkowienko-1024x700.jpg>) Thanks to the internet, we now obtain information, make purchases, and communicate with each other in ways that are dramatically different than they were only a few years ago. In fact, the advent of email, eCommerce, and social media has irrevocably changed how we conduct our daily lives. And the Internet of Things (IoT) extends connectivity to everyday devices such as cars, cameras, and smart refrigerators.

At the same time, the internet has had a potentially greater impact on the often-invisible systems that support the way we live. Known as Supervisory Control and Data Acquisition (SCADA) systems, they run



critical infrastructure components such as water treatment plants and gas pipelines. They include industrial processing systems that control refining and generate power, as well as systems that enable operations at critical domestic facilities, such as airports.

The internet, and particularly the Internet of things, offer significant benefits for managing these infrastructure and industrial control systems (ICS). But because these backbone systems can communicate over the internet, they can also be attacked over the internet.

SCADA Systems Exposed to Risk

Being able to access SCADA systems over the internet has some obvious benefits for government departments or agencies that oversee local or regional utilities or infrastructure. Industrial control system controllers and sensors that are connected to the internet can be controlled, monitored, and maintained remotely, even from a single location.

This ability also exposes them to risk, however, and the programmable logic controllers (PLCs) and ICSs that form the backbone of SCADA systems were not designed with cybersecurity in mind. In addition, some significant obstacles impede SCADA system component protection.

For one thing, as long as a SCADA device performs its intended function, there is little incentive to change it. Moreover, utilities and other industries rely on SCADA devices that were developed before the internet age and cannot be updated. And even if a vendor can provide a security patch, applying the patch can be a problem. A production line or oil refinery is not like a web server – you cannot just shut it down, apply the patch, and start it up again. Down time can cost millions of dollars a day, and every change in configuration must be tested before being put into a production environment.

SCADA Threats are Real

It's easy to dismiss sensational headlines or doomsday scenarios as fantasy. While attacks on SCADA systems could result in some catastrophic scenarios, in most cases the damage would be limited.

However, attacks with serious consequences are possible. As demonstrated in this video, it would be relatively simple for an attacker to execute a man-in-the-middle attack if an ICS network is compromised. And such an attack could, for example, cut off electricity to an entire city while the human-machine interface in the control room continues to reflect normal operation.

Although hacking industrial control systems requires exceptional technical knowledge, the source code for many potential exploitations, including state-sponsored Stuxnet and various tools leaked from the NSA, is freely available on the web. In addition, attackers work around the clock, playing with existing code and working on innovative ways to infiltrate and exploit SCADA systems.

Reducing Risk and Protecting SCADA Systems

It is simply not feasible for a government department to replace every PLC and ICS device with a new version designed with security in mind. Thankfully, risk can be managed and reduced. Risk management and reduction requires a holistic approach to security.

1. Map the Network

The first step is to map the network. Identify how networks are connected or segmented, and create an accurate picture of the entire environment.

2. Identify Assets

Next, develop and maintain a complete inventory of devices that are connected to the network. Make sure new devices can be protected and the inventory updated in real time.

3. Identify Critical Systems

Prioritize assets. When considering which assets are more critical, consider both the intrinsic value of the asset and which assets are most likely to be targeted by attackers. It is also a good idea to hire an outside company to conduct a security audit and penetration test to help identify any gaps in security.

4. Reduce Your Attack Surface

Remove unnecessary devices and disable unnecessary services to minimize potential attack vectors and reduce the overall attack surface.

5. Patch and Update

Finally, to the extent possible, identify any available patches or updates for your devices and applications and deploy them.

Protect Your SCADA Systems

SCADA systems are the backbone of critical infrastructure. The internet age has enhanced the functionality of SCADA systems but has also exposed them to new risks. The key to defending SCADA systems effectively is to be aware of potential issues and plan ahead.

Aleksander is a cybersecurity expert with more than 20 years of experience in the U.S., U.K. and Europe. He and his team of security consultants at Spirent SecurityLabs work with global companies, states, and local municipalities and agencies to protect their critical data, intellectual property, and reputation.

Tags: Smart Cities & Technology , Commentaries , Smart Cities & Technology , Commentary

(<https://www.americancityandcounty.com/>)

© American City and County 2019. All rights reserved.

About Us (<https://www.americancityandcounty.com/about-us-2/>)

Contact Us (<https://www.americancityandcounty.com/contact-us-2/>)

Cookies Policy (<http://corporate.knect365.com/privacy-centre/our-cookie-policy/>)

Privacy Statement (<http://engage.informa.com/privacy-statement/>)





Terms of Service (<http://engage.informa.com/terms-of-service/>)

Related Links

IWCE's Urgent Communications (<http://urgentcomm.com/>)

IWCE Expo (<http://www.iwceexpo.com/>)

Follow us

 (<https://www.linkedin.com/company/american-city-and-county/>)  (<https://twitter.com/AmerCityCounty>)
 (<http://www.facebook.com/AmericanCityCountyMag>) 
(<https://www.americancityandcounty.com/feed/>)