datacentrix

A comprehensive guide to HMI and OT protection

By Andre Froneman
OT Solutions Specialist at Datacentrix

In the realm of industrial cybersecurity, understanding potential attack vectors is vital for developing robust defence strategies.

Human Machine Interfaces (HMIs) in industrial environments are critical for operational oversight, but their web-based nature can make them a target for cyber threats. Hackers often employ traditional IT reconnaissance and exploitation tactics to compromise web-based HMIs, which can serve as entry points into an organisation's operational technology (OT) environment.

This process could start with the use of intelligent monitoring software solutions to look for web-based HMIs to exploit leaked virtual private network (VPN) credentials. Having identified the target, the next step involves identifying open ports using a network scanner solution to help discover hosts, services and operating systems on the network.

Using any of the 154 known exploits for virtual network computing (VNC), attackers will most likely try and extract the password, moving laterally on the system or – worst-case scenario – deploying destructive ransomware.

Depending on the network, security and server topology that lie behind the HMI, attackers will use this to pivot to many areas of the network.

> Human Machine Interfaces (HMIs) in industrial environments are critical for operational oversight, but their web-based nature can make them a target for cyber threats. Hackers often employ traditional IT reconnaissance and exploitation tactics to compromise web-based HMIs, which can serve as entry points into an organisation's operational technology (OT) environment.

Advanced attackers will find a quick way to access un-monitored areas like building management systems, CCTV, access control and industrial internet of things (iIOT)/ IOT networks so they can enjoy more time undetected in the network.

In real-world scenarios, unauthorised access to SCADA/ICS systems could have severe consequences, including disabling critical systems, manipulating industrial processes and even potential physical damage or danger.

> As industrial control systems and connected devices expand, so do the potential vulnerabilities and risks. This makes cybersecurity a priority within this environment. By implementing these layered security strategies, organisations can establish a robust and resilient infrastructure that is well-equipped to adapt to and withstand future cybersecurity challenges.

Mitigation strategies for HMI security

Securing HMIs is essential for protecting OT systems and, with a proactive cybersecurity approach, businesses can safeguard their critical infrastructure against evolving cyber threats. Thus, focus should be placed on:

1. Regularly assessing the security of industrial systems. Companies should not be satisfied with IT to OT traversal testing only. Everything, including OT, iIOT, IOT, building management systems, CCTV, access control and Programmable Logic Controllers (PLC) code, should be tested.

2. Putting robust network segmentation into action. Network segmentation according to the IEC 62443 best practices for cybersecurity, or a framework of choice, should be rolled out.

3. Keeping systems updated. Considering operational constraints, organisations should ensure that OT endpoint detection and response, intrusion prevention and intrusion detection systems are verified and kept up to date to safeguard their OT operations using OT-native Zero Trust solutions.

4. Developing incident response plans. Effective response plans must include restorability of HMIs, PLC code, historian databases, engineering workstations and other 'IT' services associated with the production line.

5. Fostering a culture of cybersecurity awareness. People are the first line of defence in any organisation. It is therefore critical that companies foster a culture of cybersecurity awareness within their shop floor workforce, partner ecosystem and OEMs.

6. Testing HMIs in pre-production staging. Using offline security scanning solutions, companies should test HMIs in pre-production staging to create a comprehensive security overview. These vulnerability management solutions are also available as a service and offer third party security certificates confirming that HMIs are malware, virus and supply chain safe.

7. Implementing OT endpoint protection and remediation software: Deploying purpose-built OT security solutions that provide comprehensive endpoint protection for industrial control systems (ICS) and HMIs. These solutions should include asset discovery and inventory management, vulnerability assessment and management, as well as allow application behaviour, file integrity monitoring and centralised security policy enforcement. The system must provide real-time threat detection and response capabilities alongside OT-specific malware protection that functions without requiring signature updates.

As industrial control systems and connected devices expand, so do the potential vulnerabilities and risks. This makes cybersecurity a priority within this environment.

By implementing these layered security strategies, organisations can establish a robust and resilient infrastructure that is well-equipped to adapt to and withstand future cybersecurity challenges.

A proactive, comprehensive approach to cybersecurity – from securing HMIs to fostering awareness and rigorous testing – ensures that critical industrial systems remain protected, safe, and resilient in the face of evolving cyber threats.

For more information contact Elzette du Preez on edupreez@datacentrix.co.za