SUPPLY AND DEMAND

Ilan Barda *reveals how organisations can stop cyber attackers exploiting weaker supply chains to breach higher value and better protected targets*

Many critical environments within energy, water and petrochemical are proud of their air-gapped approach to cyber security. However, at an organisational level there is often a lot more accessibility than is assumed. Over the last few months, several cyberattacks have highlighted potentially weak links in the chain that attackers are increasingly looking to exploit. The most recent was a major attack on water treatment facilities in Israel that points to a likely third-party contractor being breached and providing reconnaissance data that allowed hackers to target the contractors' water industry customers. These oblique attacks that aim to reach a target through first breaching a partner or proxy are a major concern. And beyond just technology, organisations are increasingly looking at how they manage partner relationships to ensure that a third-party supply chain weakness does not result in a breach that is potentially difficult to prevent and harder to spot.

In early April, leading Israeli news site YNET reported that water and wastewater facilities in the country were subject to cyberattacks. According to the article, officials at the National Water Authority stated that they had received several reports regarding cyberattacks on Operational Technology (OT) systems prompting all water providers to change passwords to operational systems and to harden internet-facing connections to operational environments. OT is a broad descriptor for the hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events that is common in Industrial Control Systems (ICS) such as a SCADA System. It is believed that a malicious actor had gained initial access remotely to some elements within an OT environment and had established its presence to access various network elements including the SCADA server, Historian or others.

There are several potential options for this initial access breach. Most local water supply and waste-water facilities are small sites and in Israel, most of them are connected via cellular-based communication to the internet for maintenance and other purposes. The cellular routers at each site are rarely hardened in terms of password control, disabling unsecure management interfaces and public facing IP address. It is believed that cyber-criminal activity had been conducted remotely by exploiting the vulnerabilities of such cellular modems.

Through discussions with contacts close to the situation, a likely possibility for access to this type of utility is supply chain compromise. Although forensic investigation continues, there are a number of contractors that possess sensitive data such as network diagrams and credentials to deliver the services they provide such as engineering site design, HMI and SCADA software and hardware provisioning along with routine maintenance. Some of these firms do not have appropriate cyber security posture to deal with more sophisticated attacks like targeted spear phishing. Therefore, in some cases APT and cybercriminal groups prefer to gain access to supply chain companies and leverage this access to target the end customer.

The attackers then use the breach of a contractor with credentials to remotely access these systems to legitimately gain a foothold within the seemingly secure perimeter. Because credentials are valid, systems designed to spot unauthorised access may fail to detect them and attackers now have a means to pivot from one system to another.

THE FBI HAS WARNED THAT THE KWAMPIRS RAT IS TARGETING SEVERAL GLOBAL INDUSTRIES

Vulnerabilities within software stacks are common and recent examples such as the newly discovered Ripple20, a vulnerability in a widely used TCP/IP stack has been found to compromise critical IoT devices from a wide range of fields. These include specialist software from bespoke developers through to products from multi-national corporations, including HP, Schneider Electric, Intel and Rockwell Automation that are used in vulnerable medical, transportation, industrial control, enterprise, energy (oil/gas), telecom, retail and commerce, and other industries. In this case, the Ripple20 vulnerabilities are deemed an accidental coding bug, but a potentially more dangerous issue is when cyber attackers actively target software supply chain providers. In this scenario, cyber attackers target software developers to inject malicious code or make changes to code that allows an exploit after the software has reached the customers installation.

Few organisations have the resources to perform deep examination of third-party software for vulnerabilities

In February 2020, the FBI issued a warning that the Kwampirs Remote Access Trojan (RAT), is targeting several global industries, including the software supply chain, healthcare, energy and financial sectors. Software supply chain companies are believed to be targeted to gain access to the victim's strategic partners and/or customers, including entities that support Industrial Control Systems (ICS) for global energy generation, transmission and distribution. The Kwampirs RAT has been observed by the FBI supporting targeted computer intrusions on these sectors, including supporting additional module execution on the targeted victim network, believed to enable follow-on computer network exploitation operations. The FBI noted that Engineer servers – which are used to develop and test ICS products and instruments and software development servers that maintain source code for software applications – as just two of an extensive list of targets of the Advanced Persistent Threat (APT) actor that has been conducting these attacks since 2016.

These kinds of attacks are incredibly dangerous as few organisations have the resources to perform deep examination of third-party software for vulnerabilities' or trojans that have been inserted into the underlying code base or – more commonly – the installation packages. Worse still, because these software elements are given elevated privileges to control critical devices; the potential for physical damage in areas such as water treatment can reach severe and potentially life threatening levels.

In response, a growing number of organisations within critical national infrastructure (CNI) and manufacturing are examining more use of zero trust methods of securing OT environments. The term zero trust is not a rigidly defined standard, but more a conceptual approach to IT security.

The National Institute of Standards and Technology defines zero trust as an evolving set of cybersecurity paradigms that move network defences from static, network-based perimeters to focus on users, assets and resources. A zero trust architecture (ZTA) uses zero trust principles to plan enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location, such as the local area networks versus the internet. Authentication and authorisation of both user and device are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users and cloud-based assets that are not located within an enterprise-owned network boundary. Zero trust focus on protecting resources, not network segments, as the network location is no longer seen as the prime component to the security posture of the resource.

Zero trust is still not widely deployed in the wider enterprise sector and even rarer in OT as industrial processes are highly automated and continually validating trust using an enterprise type ZTA is often impractical in many industrial use cases. Instead, utilities and manufacturing systems have traditionally preferred to air gap networks to remove outside connections. However, a 2019 study by the SANS institute still found that remote access (bypassing intended architecture) accounted for 40 percent of initial attack vector (point of entry) involved in an OT/control system security incident. However, moving to some ZTA position is possible, but still a significant project. And the conservative nature of these sectors means that change has been slow.

There are positive initiatives that are starting to be adopted by OT users and suppliers to improve security posture. For example, the IEC 62443 International Standard has proven its worth in the industrial automation environment and is one of the rare examples of a framework that is aimed at plant operators, integrators and component manufacturers, and covers all security-relevant aspects of industrial security.

The standard has been led by the IEC with significant input from the industrial sector and provides a definition of the security capabilities for system components along with a common language for product suppliers and all other control system stakeholders. Because the standard spans both users and suppliers, it simplifies the procurement and integration processes for the computers, applications, network equipment and control devices that make up a control system.

On the supplier side, major vendors such as Siemens have migrated to secure development processes and substantial technical product requirements that are implemented in compliance with the relevant parts of the IEC 62443 standard and independently certified by TÜV SÜD across its industrial automation, communication and drive technology, including industrial software.

Schneider-Electric and Rockwell Automation, two major OT suppliers, have also adopted the standard with varying levels of adherence across different parts of their portfolios. And both join a further 30 organisations as part of the ISA-GCA forum that are actively working together to promote the standard.

For users of OT in areas such as water treatment, energy and manufacturing; IEC 62443 helps organisations to reduce both the risk of system failure and the exposure to cyber threats using guidance from 14 documents divided into four groups: General, Policies and Procedures, System and Component to provide practical steps. For example, 62443-1-1 3.2.88 provides a guideline for conducting a risk assessment process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources; quantifying loss exposures and consequences based on probability. A growing range of cyber security and industrial management solutions for the industrial sector including Radiflow and KPMG are also making it easier for organisations to conduct ISA/IEC 62443 assessments and make the necessary changes to gain compliance.

Although there is no completely effective method of securing against cyberattacks, organisations within OT need to start insisting that suppliers must adhere to minimum standards such as IEC 62443. When it comes to service providers such as contractors, adherence to ISO 27001, a widely recognised specification for an information security management system offering a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes – should also start to become a minimum requirement. Organisations within OT both from the customer and supplier side are starting to stipulate adherence to these security related standards in contract terms and RFPs. This economic motivation is likely to accelerate wider adoption, which will lead to a better overall security posture and a reduction in supply chain attacks ●

Ilan Barda, founder of Radiflow is a Security and Telecom executive with 20 years of experience in the industry. Ilan has deep experience in developing secure communication equipment from his service in the Information Security division of the IDF.

There are a number of contractors that possess sensitive data that can put national infrastructure at risk