Utility Cybersecurity: Shut Back Doors to Critical Operational Systems

Cyberattacks on utilities are becoming more frequent, more successful, and more dangerous. While utilities have some of the most sophisticated and effective cybersecurity measures and protocols in place and update them frequently, they also face significant and proven vulnerabilities posed by third-party vendors.

Early in 2018, the Department of Homeland Security (DHS) and FBI issued a Technical Alert (TA18-074A)[1] warning that the Russian government is targeting the energy and other industrial sectors. Attacks were comprised of strategic, multi-stage campaigns, using techniques such as spear-phishing and staging of malware, all designed to conduct network reconnaissance and collect information pertaining to industrial control systems (ICS). The ultimate goal for these threat agents: reach a point where they can throw switches.

Before this alert was released, Symantec issued its own report on these campaigns, detailing what it referred to as the re-emergence of a cyberespionage group known as "Dragonfly," which had been targeting the energy sector since at least 2011.[2] After a period of relative quiet, the Dragonfly group re-appeared in 2015, continuing its efforts to carry out campaigns aimed at learning how utility facilities operate and maneuvering its way towards gaining access to the ICS themselves. Of note, Symantec had previously described Dragonfly as "technically adept and able to think strategically."[3] It continued with: "given the size of some of its targets, the group found a 'soft underbelly' by compromising [utility] suppliers, which are invariably smaller, less protected companies."

[1] United States Computer Emergency Readiness Team, Alert (TA18-074A), "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors (2018). https://www.us-cert.gov/ncas/alerts/TA18-074A

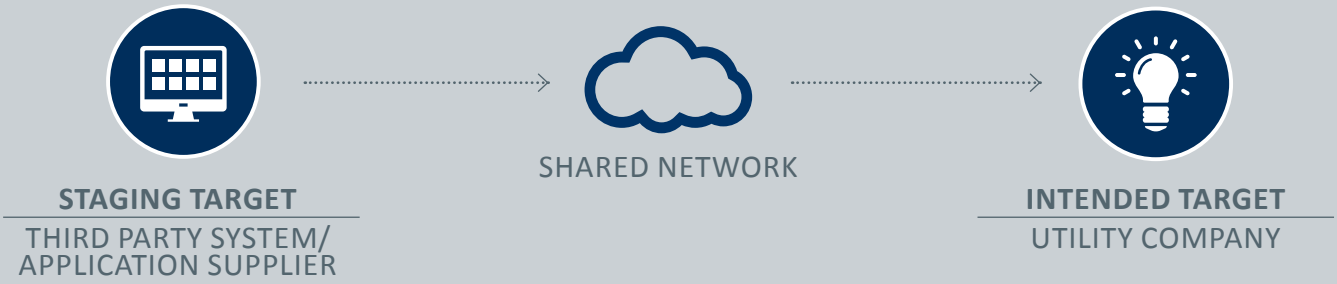
[2] https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks October 20, 2017.

[3] "Dragonfly: Western Energy Companies Under Sabotage Threat," Symantec blog, June 30, 2014. https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat-energetic-bear

AVTEC

Phone: 1.803.358.3600 • avtecinc.com
100 Innovation Place • Lexington SC 29072 USA

As detailed by the DHS and FBI, these threat actors target two distinct categories of victims—staging and intended targets. Hackers begin by exploiting the systems and applications provided by trusted third-party suppliers—staging targets—using any opening as a pivot point to gain direct access to utility systems, the intended target. Utilities use many applications, components, and systems that are developed, installed, and upgraded by third-party vendors, including mission-critical communications technology. These communication systems often share a common network that is necessary not only for day-to-day operations, but also for resiliency and restoration processes. Protecting these third-party, mission-critical communications systems must be a consideration when assessing and managing a utility's overall cybersecurity posture.



Systems Security

While the task is daunting and there are many areas for concern, there are multiple, achievable ways to provide systems with secure operating environments. This paper identifies some of the energy-focused ones for consideration.

Security Awareness Training

The best defense against any cybersecurity attack starts with the front line of an organization and extends to business partners. Employees, contractors, and third-party suppliers must be trained to be vigilant regarding system and application use, maintenance, and physical access. These individuals are the ones most likely to be targeted and are also the people who, when properly trained, will be first to notice an attempted intrusion. Training should be performed systematically and tailored to align with business roles to ensure best practices for cybersecurity are always top of mind. The objective for training should be to instill a culture of cybersecurity, one where individuals are vigilant about recognizing potential threats and equipped with processes and procedures to fend them off.

AVTEC
Phone: 1.803.358.3600 • avtecinc.com
100 Innovation Place • Lexington SC 29072 USA

Supply Chain Risk Management

On October 18, 2018, the Federal Energy Regulatory Commission (FERC) approved the supply chain risk management reliability standards, CIP-013-1, submitted by the North American Electric Reliability Corporation (NERC) in response to the commission's directives from Order No. 829.[4] The purpose of CIP-013-1 is to mitigate cybersecurity risks in a utility's supply chain, including communications technology and ICS. Compliance with CIP-013-1 requires the development of one or more plans to address four objectives for high- and medium-impact Bulk Electric System (BES) cybersystems:[5]

1. Software integrity and authenticity.
2. Vendor remote access.
3. Information system planning.
4. Vendor risk management and procurement controls.

Before procuring any mission-critical system, including a communications technology, energy companies should closely examine their vendors' security protocols, including how often measures are updated to counter evolving threats. Vendors must be held accountable to ensure that software, hardware, and other components have not been tampered with or maliciously infected before arrival onsite. Specific security requirements, expectations, and controls should be included in a Statement of Work (SOW), contracts, and Requests for Proposals (RFPs). Another alternative is to tie payments to the validation of implemented security controls and features. This linkage will motivate vendors to be vigorous in their compliance, tightening their own security and achieving higher standards through creative, enhanced solutions.

For hardware and software designed and manufactured overseas, vendors should be required to utilize tamper tapes to secure boxes and track all shipments end-to-end using a certified signature method. The goal is to create an audit trail and ensure the shipment never deviates from its safe route to its destination. Even with strict controls, it is a challenge for the average vendor to accomplish the objectives because of inadequate processes or controls. Unfortunately, non-compliant vendors may be the only option available. Nonetheless, utilities should push back and demand vendors do more to reduce the likelihood of breaches and exploitations.

Before granting system access to a vendor, complete a thorough screening and contract process. Ensure vendor employees have gone through background checks. Also, use only secure connections from the vendor's network. The vendor must be able to adhere to the utility's corporate security policy. A review of the vendor's security policy and controls may be necessary to find out how well the vendor is going to be able to secure the utility's data and the interconnections between both systems. Only vetted and authorized personnel should be allowed onto the utility's network.

This vendor-focused activity leads to Vendor Risk Management and Supply Chain Risk Management efforts at a corporate level, which is now recommended by the National Institute of Standards and Technology (NIST) through its published guidance document, SP 800-161 "Supply Chain Risk Management Practices."[6]

[4] U.S. Federal Energy Regulatory Commission, Order No. 850, Supply Chain Risk Management Reliability Standards (2018). https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf?csrt=15773227531081670129

[5] North American Electric Reliability Corporation, CIP-013-1, Cyber Security – Supply Chain Risk Management (2017). https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf

[6] National Institute of Standards and Technology, Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, (2015). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

Testing of Systems and Applications

After a successful implementation of security awareness training and supply chain risk management, the next step is to test the mission-critical systems and applications in a controlled environment before deploying into the production network. Mission-critical communication systems should be set up and tested using various automated and manual tools to validate that security requirements, expectations, and controls are met. Scenarios such as misuse testing—acting like a user—are employed to provide some confidence that the application will behave correctly under stress-based conditions. These tests are sometimes performed by external organizations under the term, "red team." Vulnerability testing, looking for common security weaknesses, penetration testing, and acting like a hacker should be considered at this phase. Any discovered vulnerabilities should be noted and communicated to the appropriate vendor. If the vendor cannot immediately resolve the issue, then request the vendor create a Plan of Action and Milestones (POA&M) item, including a secure workaround until the vulnerabilities are fixed. The ultimate objective is to introduce "clean" systems and applications to the production environment to establish a clean baseline.

Ports, Services, and Protocols Management

Utilities should require vendors to provide architecture and networking design of a mission-critical communications system. It should include all hardware and software connections and state the necessary source and destination ports, including port ranges, and services and processes tied to each port required for business operations. Only the required logical network ports and services deemed necessary should be utilized. It is essential to identify approved ports and services to help network defenders manage network traffic through firewalls and intrusion-detection and prevention systems. The best practice is to logically disable/uninstall unnecessary ports and services on all devices within the production environment to mitigate unauthorized access.
In addition, a packet-filtering firewall should be leveraged to look at destination and source addresses, ports, and services requested. At the network layer, only the approved whitelisted ports and services should be accepted. All unauthorized incoming and outgoing traffic should be disabled or blocked.

AVTEC

Phone: 1.803.358.3600 • avtecinc.com
100 Innovation Place • Lexington SC 29072 USA

Security Patch Management

Every applicable major and minor release of security patches and firmware updates from third-party vendors should be tracked and evaluated expeditiously. Test security patches and firmware updates in a controlled environment prior to full production deployment. Confirm that each new device is fully patched before deploying to the production environment. Utilize an application and system scanning tool to validate that security patches and firmware updates are up-to-date.

There is an intricate balance with patch management—security verses availability. There are times when a security patch could impair the behavior of the system or cause downtime. A secured system that is not fully functioning or offline is useless. Meanwhile, an available system with security holes may be subject to various threats. Utilities and their suppliers should be able to assess risk versus reward as well as potential compensating measures. Not all vulnerabilities have related patches, so system administrators must not only be aware of applicable vulnerabilities and available patches, but also of other methods of remediation (e.g., device or network configuration changes, employee training) that limit the exposure of systems to vulnerabilities.

Malicious Software Management

Malware attacks come in many insidious forms, from viruses, worms, and Trojan horses, to hybrids and exotic programs. There are various malware solutions on the market. Choosing the right solution for the appropriate environment can be an overwhelming task. The right solution should at least provide standard and embedded system and application protection and must be updated to receive and distribute the latest definitions. Additionally, the solution should have the option of either agent or agentless deployment. For embedded devices that do not support malware solutions, it is essential to have a layered approach—firewall and intrusion detection and prevention systems. These compensating controls will help cover and reduce potential exposure. Some mission-critical communication systems may not be able to run a malware solution due to an adverse impact on the system and application. In this case, the best option is to exclude the identified and approved directories and executables to maintain a host-based malware solution.

Configuration and Baseline Profile Management

Configuration management should be instituted to reduce unauthorized changes and record implemented changes. Utilities should establish a Configuration Control Board (CCB), which is typically comprised of business unit and information technology managers. The CCB is the organizational group responsible for overseeing all configuration changes to active systems, including approving, disapproving, or deferring a request, managing costs, and minimizing downtime. When a change is presented to the CCB for approval, the system and application owners should be notified before authorization. This allows for review and evaluation of the proposed change to be conducted. After deployment, all parties involved in any update—including vendors, users, and application owners—should be notified to allow time to provide information and training to the operators and support staff affected by the change. Whenever unscheduled changes must be implemented, and time does not allow for a prescribed protocol to be followed, those changes should still be managed and controlled. A solid change-management process that includes proper vetting will help minimize changes that could have an adverse impact on the production environment.

A mission-critical communications system should not only go through change control, but a baseline profile should be established for each device and application. It is important to utilize an automated tool to have an established baseline structure. If any change deviates from the baseline without an approved change control, then the tool should flag such incidents and a specialized team should carefully investigate. If it's a false positive, accept those changes as the new baseline. If not, remove the change and perform testing to ensure the system and application have not been adversely altered or compromised. Validate that both the system and application are in a secure state and working appropriately.

System Access and Alert Notification

Access control begins and ends with an organization's internal policy. The appropriate policy should support local domain or Active Directory authentication. The appropriate data and asset owners should identify approved users and determine access, permission, and restrictions for user roles assigned to a given asset. User access should be restricted based on roles and responsibilities. Role-based access helps prevent unauthorized access to critical and important applications and systems. Further, implementing strong password complexity settings, secure connection, and two-factor authentication will help safeguard the confidentiality and integrity of system and application access. An important aspect of system and application access that is often overlooked is the removal or adjustment of access rights and default credentials. When an employee has been transferred or terminated, or the status of a vendor has changed, the access to electronic systems, applications, and physical facilities should be reviewed, adjusted, and disabled/removed in a timely manner. Also, remove or change default usernames and passwords tied to systems and applications to eliminate the possibility of exploitation.

A Simple Network Management Protocol (SNMP) Manager and SNMP Agent should be installed in the appropriate environment to query, collect, and send system and application information. Whenever a notification trap is triggered (disk capacity, hardware failure, system offline, successful and unsuccessful authentications, password threshold, error messages, etc.), an alert should be sent to the appropriate groups and/or personnel. The alert notification allows system and application custodians to be proactive and help defend the physical and logical security boundaries.

AVTEC

Phone: 1.803.358.3600 • avtecinc.com
100 Innovation Place • Lexington SC 29072 USA

Application Security

Applications, especially web applications, are vulnerable to cyberattacks. The primary problem with an insecure application usually lies in the roots of the software development foundation and process. That's why utilities should expect their mission-critical communication system vendors to participate in an ongoing audit and compliance process for their systems. A vendor that has participated in vulnerability testing, penetration testing, black-box testing, or white-box testing has a proven level of due diligence.

Before procuring an application, energy companies should request NERC-CIP, NIST 800-53, and other relevant security compliance or certification accreditation. Without knowing the status of the application source code and pre-existing vulnerabilities, software defects, and logical flaws, the organization opens their network infrastructure for potential exploitation.

Additionally, utilities should review and use standards that are accepted and instituted for application security such as the Open Web Application Security Project (OWASP). This project is an open, worldwide security community dedicated to enabling organizations to develop, purchase, and maintain applications and application programming interfaces (APIs) that can be trusted. The following page provides an overview of OWASP's Top 10 Application Security Risks, as produced in December 2017, with the general causes for each risk.[7]

[7] "Category: OWASP Top Ten Project," Open Web Application Security Project (2017). https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

AVTEC

Phone: 1.803.358.3600 • avtecinc.com
100 Innovation Place • Lexington SC 29072 USA

OWASP's Top 10 Application Security Risks

A1 Injection

Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A2 Broken Authentication Exposure

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

A3 Sensitive Data

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged using a browser.

A4 XML External Entities (XXE)

Attackers can exploit vulnerable XML processors if they can upload XML or include hostile content in an XML document, exploiting vulnerable code, dependencies, or integrations. These flaws can be used to extract data, execute a remote request from the server, scan internal systems, perform a denial-of-service attack, as well as execute other attacks.

A5 Broken Access Control

Exploitation of access control is a core skill of attackers. Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) tools can detect the absence of access control, but cannot verify if it is functional when present. Access control is detectable using manual means, or possibly through automation for the absence of access controls in certain frameworks. When they gain access control, attackers can act as users or administrators with the ability to use privileged functions and create, access, update, or delete every record.

A6 Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up-to-date

A7 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser that can hijack user sessions, deface web sites, or redirect the user to malicious sites.

A8 Insecure Deserialization

Exploitation of deserialization is somewhat difficult, as off-the-shelf exploits rarely work without changes or tweaks to the underlying exploit code. The impact of deserialization flaws cannot be overstated. These flaws can lead to remote code execution attacks, one of the most serious attacks possible.

A9 Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

A10 Insufficient Logging and Monitoring

Exploitation of insufficient logging and monitoring has caused nearly every major incident. Attackers rely on the lack of monitoring and timely response to achieve their goals without being detected. Most successful attacks start with vulnerability probing. Allowing such probes to continue can raise the likelihood of successful exploitation to nearly 100 percent. In 2016, identifying a breach took an average of 191 days — plenty of time for damage to be inflicted.

AVTEC

Phone: 1.803.358.3600 • avtecinc.com
100 Innovation Place • Lexington SC 29072 USA

OWASP developed this list to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses. This guidance and these basic techniques will help protect against high-risk problem areas.

To this extent, application development frameworks, such as the OWASP-developed Software Application Maturity Model (SAMM), have been developed, instituted, and implemented by many software and systems companies over the past few years, providing a guide for software security strategy, evaluation, and measurement. System and application security, however, must be an ongoing process, not a destination. There is no bulletproof solution to completely protect or isolate systems and applications from being compromised by threat actors. To better manage and protect systems and applications, it is essential to examine governance and administrative policies, operational and technical risks, and implemented controls. With a good foundation and understanding of risk and control management, organizations can better protect, mitigate, and manage cybersecurity risks.

Above all, the implementation of a comprehensive security ecosystem starts with a paradigm shift throughout the organization, from senior officers to end users. Without proper management support and a culture of continuous improvement that includes ongoing security awareness training, organizations will struggle and likely fail to defend their systems and applications.

The internal and regulatory pressure to protect systems and applications is already enormous. As the public learns more about emerging threats and vulnerabilities, they put on more pressure for an urgent response. Businesses and organizations then push vendors and manufacturers to quickly develop security patches and hotfixes to protect or mitigate system and application holes and exploitations. While the urgency is real, it's easy to overreact in such an environment, resulting in quickly developed solutions that can cause adverse impacts on hardware and software. Software repairs require testing and review of the patches themselves. Installing these software components quickly can, and often does, lead to other software, hardware, and system deficiencies and weaknesses that are open to unforeseen compromise. Therefore, it's important for utilities to follow a methodical development, testing, and implementation process, such as the OWASP-based SAMM, to mitigate the introduction of any other potential vulnerabilities.

Web Application Development

Applications running with web enablement make up most of the development in today's rapidly advancing technology market. Multiple lessons have been learned since the World Wide Web was invented in 1989 with respect to conducting secure transactions and communications. Some of these lessons include such things the deployment of web-application firewalls (WAFs) between web servers and the internet, and validating inputs and testing by ensuring inputs are within the expected range.

Other advancements include handling errors and exceptions with invisibility to the user so motivated attackers cannot get additional information about potential weaknesses in the application, and creating self-monitoring software that monitors the user's activity to flag unusual events and actions.

Development Life Cycle

Mission-critical communication technology vendors may have different software development life cycles (SDLC), but the goal of any energy organization is to understand pre-existing software weaknesses and mitigation steps. Applications are usually compromised because of poor programming practices. Utilities should implore vendors to use secure software best practices like DevOps and other secure techniques to decrease the chances of repeating known software bugs, defects, logical flaws, and vulnerabilities. Establishing application security requirements, designing application security architecture, implementing standard security controls, continuously monitoring and improving the secure development life cycle, and enforcing application security education will create a more secure software ecosystem.

Find out which programming language each software vendor or development organization uses. There are many different software languages and code development techniques, each with known strengths and weaknesses. Ensure that all software developers receive training in writing secure code for their specific development environment and language.

AVTEC

Phone: 1.803.358.3600 • avtecinc.com
100 Innovation Place • Lexington SC 29072 USA

Application Testing

Utilities and their suppliers should use these four recommended application testing methods to ensure the safety of the software used in especially critical energy sector applications:

1. **Static Testing of Software (SAST)**, which involves software code reviews, line-of-code logic reviews, and automated software exams that search for errors in the logical structures and flaws in the implementation of routines.

2. **Dynamic Testing of Software (DAST)**, which checks the software in action to see if it actually works and how well it produces the expected outcomes.

3. **Testing the application while connected to other software**, which will reveal how the application performs when connected to and communicating with other applications and output devices. All components and applications need to be reviewed and evaluated to show operational status, expected behaviors, and expected outputs.

4. **Production level testing of the application** must occur before going live. Regulators usually require operational testing of applications and systems to show both risk management and due diligence in employing new components. This type of testing is conducted as the last step prior to the application being deployed in the production environment. This level of testing often uncovers communication errors or deficiencies in design or development of software that supports equipment deployed in the field.

AVTEC

Phone: 1.803.358.3600 • avtecinc.com
100 Innovation Place • Lexington SC 29072 USA

Conclusion

The DHS and FBI have reminded the energy industry that it continues to be a prime target for cyberattacks. Hackers have proven that, under the right circumstances, they can find a path into staging targets, gather info, and move on to intended targets. And they're relentless in their efforts to break through any barriers erected to keep them out.

With this as the backdrop, it's fair to say a utility's cybersecurity posture is only as strong as its weakest link. With third-party suppliers and vendors increasingly being used as staging targets, they have the potential to become this weak link unless they are fully vetted and can demonstrate they are able to meet cybersecurity requirements for systems and applications. Consider this: All it takes for a serious breach is for a hacker to learn the password of a vendor's employee who has access to the system. And there are, unfortunately, many other opportunities.

All energy organizations and vendors must protect and defend their technologies, systems, applications, and communications with even more vigor, imagination, intelligence, and resources than the hackers who are attempting to break in. From the smallest suppliers to industry leaders, all systems and applications must be protected and secured starting with how they are built, transported, and installed through how they are used, maintained, and updated. The focus must be on all mission-critical systems and applications, including those used for communications.

AVTEC

Phone: 1.803.358.3600 • avtecinc.com
100 Innovation Place • Lexington SC 29072 USA