The Link Between Government Cybersecurity and Supply Chains

MARKET TRENDS REPORT

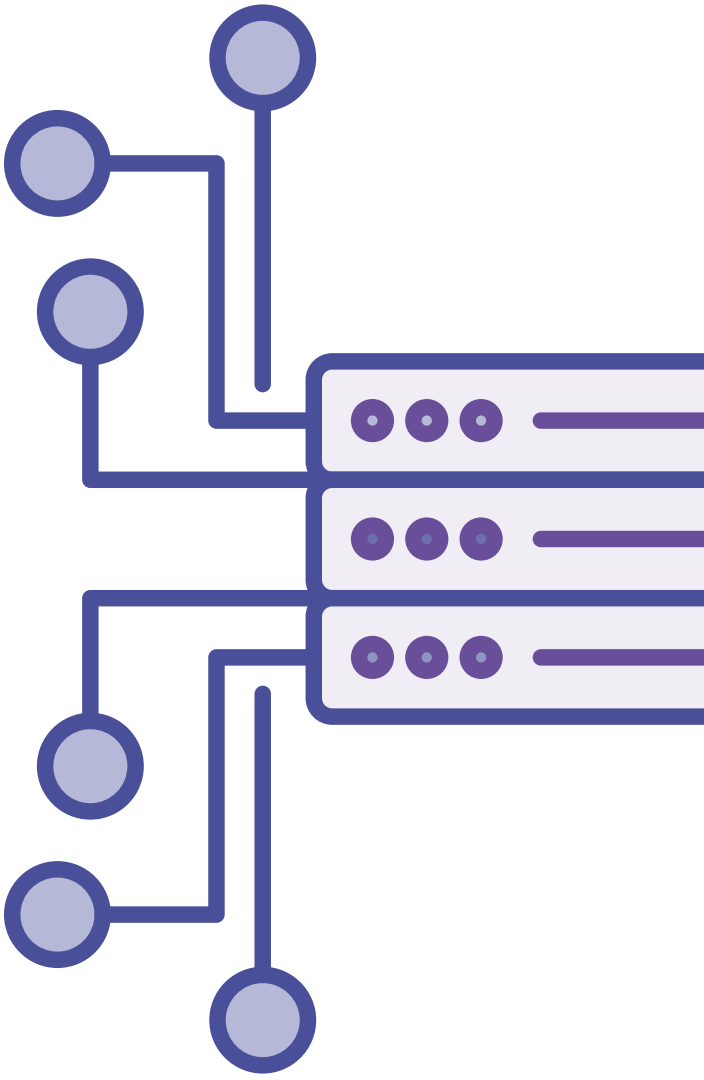
govloop

Alcatel·Lucent
Enterprise

Introduction

Cyberattacks like the SolarWinds incident have raised questions about the security of government technology supply chains. At the same time, President Joe Biden's executive order (EO) on cybersecurity has established IT supply chain security as a new national priority. In this environment, federal agencies must be assured of the security of their network switches.

As the central piece of hardware that connects devices on a network, the switch plays a key role in supporting cybersecurity. Simultaneously, vulnerabilities within switches represent a potential gap in agencies' cyber defenses. To that end, the federal supply chain for network switches is a key concern.



From the rise of remote work to the explosion of internet of things (IoT) connections, network expansions make it doubly important for agencies to ensure a robust and secure supply chain for their switches.

To learn more about how agencies can improve their cybersecurity with network switches, GovLoop developed this resource with Alcatel-Lucent Enterprise, a telecommunications equipment provider. This report explains how protecting their IT supply chains can ultimately deliver secure network switches to agencies.

By The Numbers: An Expanding Threat Landscape

A rising wave of cybersecurity incidents demonstrates the need for secure network switches:

59%

of organizations worldwide (including **61%** in the U.S.) have experienced a data breach caused by a third-party vendor.

97%

of firms have been impacted by a cybersecurity breach in their supply chain.

65%

of Americans believe the federal government should take action to help fix the problems currently affecting the U.S. supply chain.

>28,000

cyberattacks against the federal government were recorded in the most recent tally.

$200 million

was allocated to cybersecurity hiring in The American Rescue Plan.

$18.3 billion

is the estimated cybersecurity spending by the federal government .

$10 billion

is the amount the federal government will spend on continuous diagnostics and mitigation.

Securing the Supply Chain for Network Switches

The Challenge: Mitigating Risks

In the face of an unreliable supply chain for network switches, agencies struggle to mitigate risk. Given the ever-evolving cyberthreat landscape — with both state-sponsored and non-state bad actors launching incursions — lack of access to secure switches presents a significant vulnerability.

Legacy switches, meanwhile, are often insecure and vulnerable to supply-chain exploits. Common switch-based attacks may include Address Resolution Protocol spoofing, Spanning Tree Protocol attacks and exploits that work through the media access control address tables or content access memory, among others.

Supply-chain exploits also threaten legacy network switches. For example, there are times when bad actors are capable of altering a network's underlying operating system software.

"That was the SolarWinds problem," said Brian Wollak, Senior Manager, Solution Architecture at Alcatel-Lucent Enterprise. "Working within the supply chain, bad actors were able to insert malicious code from the inside."

Network switch hardware can likewise be compromised during production and transportation, like when malicious chips are embedded in the circuitry.

The rise of remote work and the growing IoT footprint can additionally magnify the impact of these vulnerabilities.

"As long as the user has the right login, they can get on the network," Wollak said. "But you don't know what device they are on and whether that is a trusted device."

Through insecure network switch supply chains, malicious actors can compromise sensitive constituent data about topics like health and finance. Moreover, they could exploit switch vulnerabilities to interrupt mission-critical government operations, putting the public's safety and even national security at risk.

The Solution: Securing Network Switches

Agencies need a reliable supply of secure network switches. What characterizes a secure switch? One key element is secure code.

"You need independent testing of the operating system in the firmware — specifically, independent verification and validation, or IV&V," Wollak said.

IV&V means that the software undergoes rigorous evaluation by a third party other than the network switch's vendor. This evaluation should be conducted after the code is compiled and should encompass penetration and information assurance testing. Any vulnerabilities that surface during this process must be analyzed and remediated.

A secure switch will also be hardened against efforts to exploit memory location. It is common for attackers to identify the layout of a switch's memory and exploit it.

"Typically, your memory locations are known," Wollak said. "And if I know where the vulnerability is on a particular operating system from a particular manufacturer, that same vulnerability works for every single one of those thousands or tens of thousands of switches."

In a secure switch, the randomized layout of address space helps prevent such attacks. A secure switch will automatically re-assign memory space so that no two are ever the same.

"Every time the switch reboots, it effectively scrambles the way it stores everything in memory, like shuffling a deck of cards," Wollak said. "Now the bad actors don't know how to attack that switch."

To meet the federal government's high security requirements, a secure-switch provider must also ensure the secure delivery of product. For example, once a third-party IV&V is completed, the code goes directly to the federal end user and not the switch's vendor. The user is thus assured that the code is the same as it was during the outside review process.

As the National Institute of Standards and Technology (NIST) now formulates policy and standards around network switches, secure switches ensure that agencies will be compliant. With a ready supply of secure switches, agencies can reduce complexity around cybersecurity operations and reduce the potential for human error.

Best Practices for Fortifying Cybersecurity

1. Embrace Zero-Trust Security Agencywide

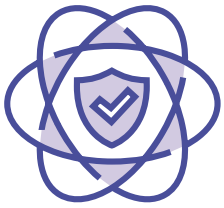
Zero-trust security assumes that networks are now perimeterless and must not trust any computing entity automatically. A secure switch fits this strategy, as it can enforce zero-trust security policies. The switch can also regulate what people and devices can attach to the network. Secure switches additionally extend this strategy to the supply chain because third-party IV&V effectively takes trust out of the equation.

2. Continuously Monitor Agencies' Resources

A secure switch supports the continuous monitoring of system health with built-in cybersecurity safeguards delivering ongoing protections. In IT systems, the practice of continuous diagnostics and monitoring (CDM) is a common defensive strategy. Agencies can think of secure switches as a way of implementing that same continuous-monitoring mentality within their supply chains. With assured sources of hardware and software, IT leaders can tap secure switches to apply constant vigilance to potential supply-chain threats.

3. Comply With Security Regulations

NIST has laid out a Cybersecurity Framework and is compiling policies and standards for network switches. With secure network switches, agencies get a head start on complying with the emerging standards. Secure switches are designed to uphold the highest level of cybersecurity awareness while meeting any new rules as agencies continue hardening their IT supply chains against possible incursions.



4. Leverage Trustworthy Third-Party Support

At a time when supply chains are suspect, agencies cannot rely on vendors alone to deliver critical IT components in a way that safeguards citizen data and vital operations.

Rather, outside evaluations should play a critical role in adopting any mission-critical IT components. With a reliance on third-party evaluation and testing, secure network switches offer this necessary degree of independent validation.

5. Take Operational Steps to Ensure Security

As agencies embrace secure switches, they can take additional steps to ensure the integrity of their systems. For example, agencies can apply threat modeling to identify vital or potentially overlooked testing targets. Agencies can also automate testing and utilize code-based analysis to detect hard-coded errors or exploits. Finally, agencies can implement security efforts at the operational level, such as ensuring that all users and devices are authenticated.

With zero-trust security, network switches will be locked down by default with few — if any — ready avenues of egress. Therefore, these best practices require a thoughtful implementation process in which administrators actively enable remote access and take other positive configuration measures. These precautions do not necessarily complicate switch implementation, but they do demand a higher level of rigor and attentiveness than may have been applied when implementing legacy switches.

HOW ALCATEL-LUCENT ENTERPRISE HELPS

Alcatel-Lucent's OmniSwitch® family of products delivers the zero-trust security agencies' networks demand.

To ensure a secure supply chain, OmniSwitch leverages third-party IV&V, including source code analysis, white box and black box testing by a company specializing in cybersecurity. This process eliminates many supply chain-related vulnerabilities, such as backdoor threats and embedded malware.

With third-party IV&V, Alcatel-Lucent Enterprise addresses external interfaces, including the HTTPS interface, login interface, NTP interface and others. And with Address Space Layout Randomization (ASLR), each switch boot dynamically generates a unique memory layout — denying attackers a predictable target at which to aim their exploits.

In addition, Alcatel-Lucent Enterprise ensures secure delivery of its products. Its U.S. supply-chain process enables designation of OmniSwitch models as TAA Country of Origin (CoO) USA, with all operational software loaded in a U.S.-based facility. In addition, the company performing the IV&V retains the code after validation testing and, over a secure connection, can provide the software directly to agencies.

"These methods augment and enhance the system quality-assurance activities that are employed in all our product development environments," Wollak said. "We have taken a zero-trust approach for decades, and security is always top of mind in everything we do."

Learn more: https://www.al-enterprise.com/en/industries/government/usa-federal

Conclusion

With cyberattacks on supply chains increasingly common — and with a recent EO calling for robust defenses — agencies need a ready and reliable source of secure network switches.

Secure network switches offer a means to satisfy emerging supply-chain standards and regulations. With this approach, government users can know with a high degree of certainty that both the hardware and software embedded in their switches are safe, secure and authentic.

With secure switches, agencies can alleviate supply-chain concerns around this critical IT mechanism. In turn, this leads to more rigorous cyber defenses.

"In switches, that means more than just the hardware supply chain," Wollak said. "Agencies also need to be assured of software security within their network switches."

Alcatel·Lucent Enterprise

ABOUT ALCATEL-LUCENT ENTERPRISE

Alcatel-Lucent Enterprise (ALE) delivers the customised technology experiences enterprises need to make everything connect.

ALE provides digital-age networking, communications and cloud solutions with services tailored to ensure customers' success, with flexible business models in the cloud, on premises, and hybrid. All solutions have built-in security and limited environmental impact.

Over 100 years of innovation have made ALE a trusted advisor to more than a million customers all over the world.

With headquarters in France and 3,400 business partners worldwide, ALE achieves an effective global reach with a local focus.

To learn more, visit: https://www.al-enterprise.com/en/industries/government/usa-federal or contact us: Federal@al-enterprise.com

govloop

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop