CLCT

WILLIAM & MARY LAW SCHOOL

Cybersecurity and Information Security Newsletter

Issue 15 | February 7, 2022

Table of Contents

Daniel Shin, research scientist with the Commonwealth Cyber Initiative (CCI) Coastal Virginia region, wants to hear from you! Submit any cybersecurity and information security news items or request related topics, via e-mail to dshin01@wm.edu.

This newsletter supports the mission of CCI. To learn more about CCI, including upcoming events, funded research, and news, please visit cyberinitiative.org.

The Office of Management and Budget publishes Memorandum to set forth a federal Zero Trust Architecture strategy

On January 26, 2022, the Office of Management and Budget (OMB) published OMB Memorandum M-22-09 (Memorandum) for federal agencies and other executive departments instructing them to begin implementing the federal zero trust architecture (ZTA) strategy by the end of fiscal year 2024. *M-22-09: Memorandum For The Heads Of Executive Departments And Agencies [OMB]*, available here. This Memorandum implements part of President Biden's Executive Order 14028, which was intended to improve the federal government's cybersecurity systems. *Executive Order 14028: Improving the Nation's Cybersecurity*, available here. Recognizing the need to use Cloud technology while protecting federal Information Technology (IT) and Operational Technology (OT) assets, Executive Order 14028 directed federal agencies to adopt ZTA as practically as possible. *Issue 8: CLCT Cybersecurity and Information Security Newsletter - President Biden signs Executive Order to increase information sharing*, available here.

The "Cloud" refers to an IT system that provides on-demand provisioned resources (e.g., data storage, network transfer, CPU/GPU processing) to users without the need for direct active management. *What is cloud computing?*, available here. It resides in a real-time virtual environment managed among different servers in various locations. Supported by Cloud Smart, a 2019 Federal Cloud Computing Strategy headed by OMB, federal agencies have been migrating their IT infrastructure to the Cloud. *See From Cloud First to Cloud Smart*, available here.

According to the U.S. Department of Defense's Zero Trust Reference Architecture, zero trust refers to "an evolving set of cybersecurity paradigms that move defenses from status, network-based perimeters to focus on users, assets, and resources." *Department of Defense (DOD) Zero Trust Reference Architecture*, available here. Instead of focusing on cybersecurity defenses on the barrier between the trusted, internal network and untrusted, external networks (e.g., firewalls), zero trust assumes that "no actor, system, network, or service operating outside or *within* the security perimeter is trusted." *Id. (emphasis added)*.

As such, a zero trust security model requires strict credential checking protocols for all users and devices accessing IT resources, *regardless of whether those resources are being accessed from internal or external network connections*. *Zero Trust security | What is a Zero Trust network?*, available here. In fact, the Memorandum specifically notes that the federal government's implementation of ZTA would include a shift from a single credential check at the perimeter to a "continual verification of each user, device, application, and transaction."

Implicit in the tenet of ZTA is securing against the possibility that *anything* in or outside the network could be compromised and used by threat actors as a vehicle to access secured resources. Furthermore, ZTA assumes that any user or device managed by the organization could be compromised and exploited to carry out further cyber attacks. Similar to how ship designs employ segmented and isolated watertight compartments to contain potential hull breaches at any part of the ship, ZTA focuses on potentially isolating network segments and compromised devices to protect the rest of the IT infrastructure. The need for ZTA's granular isolation feature is even more pronounced as federal IT and OT systems extend beyond government networks and to third-party-managed Cloud services.

To implement successfully the federal government's ZTA strategy, the Memorandum includes the following requirements:

- Federal agency staff will be required to use enterprise-managed identities to access resources for their work. Phishing-resistant multi-factor authentication (MFA) will be mandatory for accessing federal IT resources.
- The federal government must have a complete inventory of every device it operates and those authorized for government use. The government also will have the capability to prevent, detect, and respond to incidents on those devices using continuous device monitoring techniques.
- Federal agencies will implement encryption to all web-based traffic (DNS requests and HTTP traffic).
- Federal agencies will regularly audit all applications for compliance with cybersecurity requirements.
- Federal agencies will implement thorough data protection practices, including taking advantage of Cloud security services to monitor access to sensitive data and implement enterprise-wide logging and information sharing regarding data access.

Mandatory Encryption of All Web-based Traffic

The Memorandum also requires federal agencies to begin encrypting all Domain Name System (DNS) requests and Hypertext Transfer Protocol (HTTP) data traffic. DNS requests are made whenever a web-connecting software (e.g., web browser) asks a DNS server to inquire about the IP address of a server associated with a target domain name. *What is DNS? | How DNS works*, available here.

Anytime an application such as a web browser attempts to connect to a web service (e.g., Google's search engine) via a domain name address (e.g., google.com), the application needs the IP address associated with the domain name before it can connect to the web service. A DNS server acts like a phonebook directory for web-based applications, where it provides the associated IP address of servers associated with a domain name (similar to how a phone book provides phone numbers of listed individuals in a city). The application makes the inquiry to the DNS server before it can connect to the target web service via the provided IP address.

From a cybersecurity perspective, the issue with DNS requests is that these inquiries are transmitted in unencrypted plain text, which makes it easy for third-party applications and other computers in the network to monitor the request. Monitoring unencrypted DNS requests allows a hostile third party to eavesdrop on what online services the target computer has been connecting over time. This can provide useful intelligence for a hostile adversary who attempts to identify critical and vulnerable systems, including those managed by third-party federal contractors, to conduct a cyber attack.

The Memorandum also mandates encrypting all HTTP data traffic. HTTP is the primary protocol used by web browsers to connect to other web-based services. Not only is HTTP used to transmit hypertext webpages, but it is "also commonly used for many *[Application Programming Interface]* among servers, mobile applications, and other endpoints." *M-22-09: Memorandum For The Heads Of Executive Departments And Agencies [OMB]*, *supra* at 14.

OMB Memorandum M-15-13 (published in June 8, 2015) and DHS Binding Operation Directive 18-01 (published in October 16, 2017) required federal agencies to employ encrypted HTTP protocol, also known as Hypertext Transfer Protocol Secure, across all internet-accessible web services (e.g., publicly facing websites) and Application Programming Interfaces (commonly known as APIs). *M-15-13: Memorandum For The Heads Of Executive Departments And Agencies [OMB]*, available here; *Binding Operational Directive 18-01 [DHS]*, available here. However, the newly published Memorandum extends the encryption requirement to both public and internal government network environments.

Encrypting HTTP data traffic ensures that (1) no unauthorized third party can access the content of the encrypted communications, and (2) no threat actor can tamper and modify the content of the encrypted communication without being alerted by the original communicating parties.

While enforcing encryption protocols for publicly facing web services may be standard best practice, recent sophisticated cyber attacks targeting federal IT resources have called for a universal encryption requirement, including data communications that are conducted internally within federal government networks. For example, in December 2020, SolarWinds, a U.S. company specializing in producing IT management software, discovered a backdoor vulnerability manifested in its product platform. *Issue 6: CLCT Cybersecurity and Information Security Newsletter - The SolarWinds hack: SUNSPOT, SUNBURST, and a compromised Office 365 account*, available here. Threat actors used the backdoor vulnerability to eavesdrop for months on internal network communications of SolarWinds customers, some of whom were federal agencies. Because internal network data traffic was not required to be encrypted, threat actors behind the SolarWinds attack could read unencrypted plain-text communications inside compromised federal networks.

Once HTTPS protocols are implemented across all data traffic, federal agencies would be protected against insider threat eavesdropping as most internal network communications would be unreadable for unauthorized third parties. Although not initially requiring encryption for internal network traffic may be seen as an obvious oversight, the conventional perimeter-based network defense model (which the federal government used previously) focused on establishing a strong perimeter and "then trust that activities within that perimeter were safe." *Traditional perimeter-based network defense is obsolete—transform to a Zero Trust model*, available here. Due to the federal government's increasing reliance on third-party Cloud services and the evolving nature of insider threats, the Memorandum properly shifts the federal cybersecurity paradigm towards ZTA.

Automating Security Responses, including using Machine Learning Technologies

Although adopting the ZTA model brings several benefits, this approach may potentially yield higher management cost, specifically in the areas of security monitoring and enforcement. Continuous authentication of all actors, systems, networks, and services increases operational costs due to enhanced security checks (e.g., a user may have to login to a web-based program every six hours because of strict authentication policies set by IT administrators). A credential management authority needs to continuously scrutinize access controls, and all activities within and across networks need to be monitored for unusual behaviors.

The vast volume of monitorable activities makes it necessary to automate security monitoring and enforcement. The Memorandum refers to this approach as Security Orchestration, Automation, and Response. Realizing the need to improve security and efficiency "without causing unacceptable disruption to the daily work of the organization," the Memorandum requires federal agencies "to employ heuristics rooted in machine learning to categorize the data they gather, and to deploy processes that offer early warning or detection of anomalous behavior in as close to real-time as possible throughout their enterprise." *M-22-09: Memorandum For The Heads Of Executive Departments And Agencies [OMB]*, *supra* at 22.

Machine learning is a branch of artificial intelligence that "focuses on the use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy." *Machine Learning*, available here. Unlike traditional algorithms, machine learning techniques allow automation with high levels of adaptability to the changing environment. Many email spam filters use some form of machine learning to identify unsolicited emails, even as spammers continuously attempt to adjust their emails to get past the filters.

Machine learning has increasingly been utilized for malware detection, specifically spotting "malicious-looking" behaviors among examined programs. In that context, training the algorithm to differentiate benign program activity with malicious processes can automate the identification and isolation of suspect programs before any further pernicious activities could continue. Machine-learned behavioral-based detection has the advantage of being able to detect a novel malicious program even before security software vendors had the opportunity to document and analyze the specific malicious program. Since 2017, Microsoft's Windows Defender for Endpoint (formally known as Windows Defender ATP), an enterprise-level security platform, has been utilizing a form of machine learning-based behavior detection systems to identify and isolate suspect malicious programs. *Windows Defender ATP machine learning: Detecting new and unusual breach activity*, available here.

Within the context of securing federal IT and OT systems, the Memorandum recognizes the challenge of implementing machine learning technologies to automated security monitoring and enforcement mechanisms. Thus, it encourages federal agencies to employ "relatively simple technical approaches" until machine learning techniques can reliably be used for security automation. *M-22-09: Memorandum For The Heads Of Executive Departments And Agencies [OMB]*, *supra* at 22.

Analysis

As enterprise IT systems increasingly utilize Cloud services to support organizations' operations, the traditional perimeter-based network model has slowly been fading away. No longer are critical resources located only "inside" the network; instead, some of the critical data and web services are managed by Cloud service providers "outside" the network. While Cloud services introduce new benefits, the traditional perimeter-based network security model no longer serves as an adequate strategy to counter cyber threats. The Memorandum's implementation of Executive Order 14028 creates a much-needed initiative to build an even more secure IT and OT environment across federal agencies without sacrificing operational productivity.

Given the large scope of this government endeavor, the Memorandum may encourage private enterprise IT systems to follow and adopt the ZTA model, creating the opportunity to raise

cybersecurity standards across the entire cyber infrastructure. In turn, this may encourage a more proactive than reactive approach to managing cyber threats.

Just-passed Virginia House Bill aims to require mandatory cybersecurity and data breach incident reporting from all state and local government bodies

On January 20, 2022, Virginia state Delegate C.E. Cliff Hayes, Jr. offered House Bill 1290 (House Bill) to expand the state's cybersecurity and data breach incident reporting requirement to cover all state agencies and organizations. *HB 1290 Public bodies; security of government databases and data communications*, available here. Subsequently, the House Bill was referred to the House of Delegates' Committee on Communications, Technology and Innovations, and, on January 31, the House Bill passed the committee's vote by twelve to two, with one delegate not voting. *01/31/22 House: Reported from Communications, Technology and Innovation with amendment(s) (19-Y 2-N)*, available here. On February 7, the House Bill passed the House of Delegates by 93 to 7. *HB 1290 Public bodies; security of government databases and data communications*, *supra*. As of this newsletter's publication, the House Bill needs to be passed in the Senate of Virginia and signed by the Governor of Virginia before it becomes state law. *See Article V, Section 6 of the Constitution of Virginia*, available here.

Under § 2.2-603(G) of the Code of Virginia, only state executive branch departments were required to report any cybersecurity and data breach incidents to the state's Chief Information Officer within 24 hours of the discovery of the incident. *§ 2.2-603. Authority of agency directors. [Virginia's Legislative Information System]*, available here and archived copy available here. Although the current statute provides an important mechanism for the state government to respond to major cyber incidents involving key state agencies, the state's Chief Information Officer does not have a complete awareness of the cybersecurity incident landscape across all state and local governmental bodies.

The House Bill amends the state statute to require every "public body" to report promptly cybersecurity and data breach incidents. "Public body" includes all government agencies and institutions that derive their legal authority from the state government, including all state courts, legislative bodies, agencies, political subdivisions of the Commonwealth, governing boards of institutions of higher educations, and other organizations supported wholly or principally by public funds.

Given the strong support from the House of Delegates, the House Bill is likely to pass in the Senate of Virginia and be signed by the Governor of Virginia. If enacted into law, Virginia would have one of the most resilient and comprehensive state incident response systems in the United States.