THOMSON REUTERS
Westlaw®

The impact of the government shutdown on U.S. cybersecurity defenses and the lessons learned

By Thomas Jackson, Esq., ***Phillips Nizer LLP***

FEBRUARY 22, 2019

The Department of Homeland Security, in large part at the urging of the private sector, set up an initiative called "automated indicator sharing," or AIS, to facilitate the sharing among businesses and federal agencies and departments of threat intelligence and the identification of threat indicators.

By enabling threat intelligence-sharing in near real time, the program intends to lessen the likelihood that a cyberexploit aimed at one or a small number of agencies or companies will be executed successfully against other businesses or agencies.

No one can disagree with the notion that a government shutdown will disrupt the delivery of services to the private sector. In the case of AIS, which according to one report had more than 80 percent of its staff furloughed during the 35-day partial government shutdown, the entire initiative came virtually to a screeching halt.

The shutdown also caused a severe staff reduction at the Cybersecurity and Infrastructure Security Agency, or CISA, also part of DHS. Working with partners in government and private industry, its mission is to defend critical infrastructure against cyberattacks.

The shutdown quite literally decimated the CISA's staff just over a month after its launch, causing 45 percent or more of its cybersecurity and technical workers to be furloughed. The same was true of the Office of Intelligence and Analysis of DHS, which develops and provides threat intelligence to government agencies and the business community.

Yet another impact in the cybersecurity field was on research activities and other programs of the Commerce Department's National Institute of Standards and Technology, as well as on the NIST's ongoing development and release of standards and guidelines.

Security personnel at major public companies use the NIST's cybersecurity framework to develop initiatives and best practices to keep their networks safe and secure and to protect their critical data.

The Computer Security Resource Center, which supports government and industry by providing access to cybersecurity and information security-related projects, programs and publications, was totally shut down. The Federal Information Processing Standards' validation programs, used to develop and certify document-processing encryption algorithms and other information technology standards employed by non-military agencies and federal departments as well as government contractors, were also operating at severely reduced capacity.

It is likely that further rollouts of the DHS Continuous Diagnostics and Mitigation program, which uses a sophisticated group of tools used to identify, prioritize and support the mitigation of the risk of cyberattacks across all non-military federal departments and agencies, will be delayed.

> The shutdown quite literally decimated the Cybersecurity and Infrastructure Security Agency's staff just over a month after its launch, causing 45 percent or more of its cybersecurity and technical workers to be furloughed.

The heightened risk to government and the private sector of potential cyberattacks by rogue nations and other bad actors during the recently concluded 35-day shutdown is self-evident.

For example, in January the CISA became aware of a series of incidents among federal agencies and departments involving a well-organized campaign of Domain Name System hijacking that impacted their secure networks and sensitive data during the shutdown.

The discovery of the exploit, which, in part, was attributable to the ongoing monitoring and the sharing of actionable threat indicators among executive branch agencies, followed reports by security researchers from the cybersecurity company Mandiant FireEye showing how hackers were manipulating DNS records to divert the targets' traffic to malicious servers.

The widespread campaign, aimed at governmental bodies in North America, Europe, the Middle East and North Africa, as well as organizations in the private sector, is believed to have been carried out by operatives in Iran and closely aligned with the political interests of the Iranian government.

As part of the exploit, attackers compromised the login credentials of authorized users, allowing the bad actors to make changes in MX, NS and address records, replacing legitimate addresses with ones controlled by the attackers. MX, or Mail Exchange, records are records in the DNS that identify the mail servers responsible for delivering email to the recipient's email address. NS, or Name Server, records, also a type of record in the DNS, point the name of a subdomain (for example, info.xyzcorp.com) to a group of name servers other than the ones used for the domain name. An address record in the DNS is used to map the domain or subdomain name to the IP address of the host server.

As a result, the hackers were able to redirect user traffic and to reset the values of the DNS records to obtain valid encryption certificates for the compromised domain names and to decrypt the intercepted data.

In many cases, these kinds of threat vectors are not routinely monitored. Once a network system has been infiltrated, the wrongdoers can intercept and manipulate legitimate traffic, mount sophisticated denial-of-service attacks and slow the delivery of services.

They can also extract and accumulate credentials, emails and other information, and analyze the architecture and topology of the system and the security measures it deploys and embed malware to create backdoors that bypass normal authentication or encryption and conceal any changes that have been made.

To stem the tide, the CISA issued a rare directive to agencies, requiring them to take the following steps within 10 days:

- Audit the DNS records on all primary and secondary DNS servers for every .gov or other agency-managed domain.
- Update the passwords for any user accounts that can make changes to the agency's DNS records.
- Implement or enhance password management procedures to enforce the complexity and uniqueness of passwords and require that passwords be changed in frequent intervals.

Some experts believe the campaign was timed to take advantage of the degraded state of parts of our national security systems that can detect such exploits and notify government agencies and the private sector so that they can act promptly after their discovery.

It is likely to take more time than one might otherwise expect for the cybersecurity infrastructure to regain its footing. If a second shutdown had not been averted, government agencies and businesses would have found themselves back in the soup only weeks after the first shutdown ended.

Some believe, if there had been another government shutdown, given the likely impact it would have had on the recruitment and retention of well-qualified personnel, it might well have caused permanent damage to the national security infrastructure.

This article first appeared in the February 22, 2019, edition of Westlaw Journal Computer & Internet.

ABOUT THE AUTHOR

Thomas Jackson is a senior partner in the New York-based law firm **Phillips Nizer LLP**. He is the chair of the firm's technology practice and is nationally recognized for his work in cybersecurity, data privacy and other related fields. He can be reached at tjackson@ phillipsnizer.com.