Presidential Warning to Businesses on Cybersecurity

President Biden signs an Executive Order charting a new course to improve the nation's cybersecurity and protect federal government networks while urging the private sector to follow suit

CRA™
Transform IT
Computer Resources of America

Table of Contents

New Measures to Cybersecurity

On May 12th, 2021 President Biden signed an Executive Order to improve the nation's state of cybersecurity by protecting federal government networks. Both the public and private sectors in the U.S. have been facing a rising number of malicious cyber activity that is growing more complex each day.

There are often common causes in these incidents which can leave businesses in compromising situations and vulnerable to future attacks.

According to a Fact Sheet released by the White House "This Executive Order makes a significant contribution toward modernizing cybersecurity defenses by protecting federal networks, improving information-sharing between the U.S. government and the private sector on cyber issues, and strengthening the United States’ ability to respond to incidents when they occur. It is the first of many ambitious steps the Administration is taking to modernize national cyber defenses."

Here are the measures being taken by the administration's order:

Remove Barriers to Threat Information Sharing Between Government and the Private Sector

The Executive Order ensures that IT Service Providers can share information with the government and require them to share certain breach information. IT providers are often hesitant or unable to voluntarily share information about a compromise. Sometimes this can be due to contractual obligations; in other cases, providers may be reluctant to share information about their own security breaches.

Removing any contractual barriers and requiring providers to share breach information that could impact Government networks is necessary to enable more effective defenses of Federal departments and improve the Nation's cybersecurity.

Modernize and Implement Stronger Cybersecurity Standards in the Federal Government

The Executive Order helps move the Federal government to secure cloud services and a zero-trust architecture and mandates deployment of multifactor authentication and encryption with a specific time. Outdated security models and unencrypted data have led to compromises of systems in the public and private sectors.

The Federal government must lead the way and increase its adoption of security best practices, including employing a zero-trust security model, accelerating movement to secure cloud services, and consistently deploying foundational security tools such as multifactor authentication and encryption.

Improve Software Supply Chain Security

The Executive Order will improve software security by establishing baseline security standards for the development of software sold to the government, including requiring developers to maintain greater visibility into their software and making security data publicly available. It stands up a concurrent public-private process to develop new and innovative approaches to secure software development and uses the power of Federal procurement to incentivize the market.

Finally, it creates a pilot program to create an "energy star" type of label so the government and the public can quickly determine whether the software was developed securely. Too much of our software, including critical software, is shipped with significant vulnerabilities that our adversaries exploit. This is a long-standing, well-known problem, but we have kicked the can down the road for too long. We need to use the Federal Government's purchasing power to drive the market to build security into all software from the ground up.

Establish a Cybersecurity Safety Review Board

The Executive Order establishes a Cybersecurity Safety Review Board, co-chaired by government and private sector leads, that may convene following a significant cyber incident to analyze what happened and make concrete recommendations for improving cybersecurity.

Too often, organizations repeat past mistakes and do not learn lessons from significant cyber incidents. When something goes wrong, the Administration and private sector need to ask the hard questions and make the necessary improvements. This board is modeled after the National Transportation Safety Board, which is used after airplane crashes and other incidents.

Create a Standard Playbook for Responding to Cyber Incidents

The Executive Order creates a standardized playbook and set of definitions for cyber incident response by federal departments and agencies. Organizations cannot wait until they are compromised to figure out how to respond to an attack. Recent incidents have shown that within the government, the maturity level of response plans varies widely.

The playbook will ensure all Federal agencies meet a certain threshold and are prepared to take uniform steps to identify and mitigate a threat. The playbook will also provide the private sector with a template for its response efforts.

Improve Detection of Cybersecurity Incidents on Federal Government Networks

The Executive Order improves the ability to detect malicious cyber activity on federal networks by enabling a government-wide endpoint detection and response system and improved information sharing within the Federal government. Slow and inconsistent deployment of foundational cybersecurity tools and practices leaves an organization exposed to adversaries.

The Federal government should lead in cybersecurity, and strong, Government-wide Endpoint Detection and Response (EDR) deployment coupled with robust intra-governmental information sharing are essential.

Improve Investigative and Remediation Capabilities

The Executive Order creates cybersecurity event log requirements for federal departments and agencies. Insufficient logging hampers an organization’s ability to detect intrusions, mitigate those in progress, and determine the extent of an incident after the fact. Robust and consistent logging practices will solve much of this problem.

Information is provided by:

FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation’s Cybersecurity and Protect Federal Government Networks

https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/

Computer Resources of America is an award-winning Managed Services Provider and offers IT consulting and solutions to businesses in the NY Tri-State area. We offer complete managed IT, cloud solutions, BCDR, cybersecurity solutions, and more for SMBs across various industries. Contact us today at consultcra.com.

CRA™
Transform IT
Computer Resources of America