akerman

Practice Update

Recent Cybersecurity and Ransomware Guidance That Every Business Should Be Reviewing

June 15, 2021

By Elizabeth F. Hodge and Christy S. Hawkins

In response to the ever-increasing number of ransomware attacks, including several recent high-profile and high impact incidents, the Biden Administration has issued several alerts and guidance documents over the last month regarding steps businesses can take to prevent disruption of their operations due to ransomware and other cyberattacks. These documents are required reading for organizations in all sectors, though businesses that operate or control critical infrastructure assets should pay especially close attention. While the Administration is taking steps to prevent and respond to cyberattacks, the recent guidance makes clear that the Administration expects the private sector to do its part to limit the impact of ransomware attacks.

This practice update summarizes some of the recent guidance from the White House and the Cybersecurity and Infrastructure Security Agency (CISA) to help businesses protect themselves against ransomware.

Executive Order on Improving the Nation's Cybersecurity

On May 12, 2021, President Biden issued an Executive Order on Improving the Nation's

Related People

Christy S. Hawkins
Elizabeth F. Hodge

Related Work

Data Privacy and Security
Healthcare

Cybersecurity. The Executive Order outlines a number of steps that the federal government will take to modernize the government's IT infrastructure, including:

- Improving supply chain security by providing guidelines for how federal agencies must evaluate the software products and services they purchase;
- Deploying multi-factor authentication, endpoint detection and response, and encryption;
- Adopting "zero trust" architecture and using more secure cloud services;
- Establishing a Cyber Incident Review Board to investigate cyber incidents and make recommendations;
- Removing barriers that prevent federal agencies and vendors from sharing threat intelligence data; and
- Creating standards to minimize the damage from ransomware incidents.

While the Executive Order is directed to action by the federal government, organizations that contract with federal agencies may also feel the impact of the Order if the government insists on amending agreements to require more robust information security protections.

White House Memorandum to Corporate Executives and Business Leaders

Following the Executive Order, on June 2, 2021, the White House issued a memorandum to corporate executives and business leaders titled "What We Urge You To Do To Protect Against The Threat of Ransomware" (White House Memo). Specifically, the White House Memo encourages organizations to view ransomware not simply as a data theft risk, but as a risk to their core business operations. As such, business executives should "immediately convene their leadership teams to discuss the ransomware

threat" and review their organization's security posture and business continuity plans to ensure they have the ability to continue or quickly restore operations. The memo also urges businesses to promptly undertake the following "U.S. Government's recommended best practices" to decrease their cyber risk:

- **Implement the following best practices from the Executive Order**:
    - Use of multifactor authentication since passwords are routinely compromised;
    - Deploying endpoint detection and response to identify malicious activity on a network and block it;
    - Encryption for data at rest and in transit to render such data unusable if it is stolen; and
    - Creating an empowered security team to patch systems rapidly and incorporate threat information into the company's defenses.
- **Backup data, system images, and configurations, regularly test them, and keep backups offline.** Since many ransomware variants try to locate and either encrypt or delete accessible backups, it is imperative to keep current backups offline so the organization is able to restore its systems in the event of an attack. Also, organizations need to confirm that their backup systems actually work, preferably before a ransomware attack.
- **Update and patch systems promptly**. Software system patches are only effective if companies promptly install them. Organizations can ensure they are current in several ways, including using a centralized patch management system or a risk-based assessment strategy to support the patch management program.
- **Test the incident response plan.** As noted in the White House Memo, testing is the best way to expose gaps in an incident response plan. Testing should target the plan and the team itself, so that team members are not seeing the incident

response plan for the first time when they are tasked with responding to a critical incident.

- **Check the security team's work.** Companies should engage third party penetration testers to verify the security of systems and the ability to respond to a sophisticated attack.
- **Segment networks.** Because cyber criminals are shifting from stealing data to disrupting operations, it is critical that companies separate their corporate business functions and manufacturing and/or production operations and limit internet access to operational networks. Also, companies should identify links between these networks and develop workarounds or manual controls to ensure that mission critical system networks can be segregated and continue operating if the corporate network is compromised.

All of the recommended best practices in the White House Memo are well known and considered to be fundamental to an effective information security program. As a result, an organization that does not implement one or more of the practices should be prepared to explain why it did not do so, especially if it experiences a cyberattack.

CISA Operational Technology Guidance

In response to recent ransomware attacks targeting critical infrastructure, on June 9, 2021, CISA issued a fact sheet on the rising ransomware threat to operational technology assets and control systems (OT Guidance). Operational technology is technology that controls and monitors industrial process assets and manufacturing/industrial equipment. The OT Guidance, like the White House Memo, emphasizes that "[a]ll organizations are at risk of being targeted by ransomware and have an urgent responsibility to protect against ransomware threats." CISA further warns that critical infrastructure owners and operators should "adopt a heightened state of awareness" and voluntarily implement recommendations in the OT Guidance, including:

- **Identify Critical Processes for Essential Services.** Companies should identify all critical processes that must continue without interruption to provide essential services.
- **Effective Workarounds and Manual Controls.** Organizations should have a plan to operate when facing an attack, including developing and testing workarounds and manual processes to ensure that the critical processes identified in the preceding step can be isolated and continue to operate without access to IT networks.
- **Network Segmentation.** Like the White House Memo, the OT Guidance recommends that organizations implement "robust" network segmentation between the information technology and operational technology networks. CISA notes that even if network segmentation is implemented, some critical operational processes may still depend on business functions performed by the IT network so organizations should promptly take steps to reduce such co-dependencies.
- **Strong Backup Procedures.** The OT Guidance encourages organizations to ensure that they have backup procedures in place and regularly test them. Backups should be isolated from network connections so they cannot be accessed by ransomware. Finally, CISA recommends performing a full restore of backups from scratch to test the backup procedure and to help map previously unknown dependencies.

CISA also emphasizes that it strongly discourages paying ransoms because that does not ensure that the company's data will be decrypted or that information systems and data will no longer be compromised, and it encourages further attacks.

HHS OCR Cyber Alert

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued a cyber alert on June 9, 2021 encouraging healthcare

organizations to review the White House Memo and take appropriate action. OCR also recommends that healthcare organizations review the recent CISA alert about a critical VMware vulnerability that bad actors are attempting to exploit. OCR and CISA recommend that organizations promptly apply the available patch, even if out-of-cycle work is needed.

Next Steps

Collectively, the guidance documents specify what the federal government deems to be best practices to reduce the risk of a successful cyberattack. All companies should review the guidance documents and, if necessary, modify their data security practices and business continuity plans accordingly. Failure to take the basic steps outlined in the guidance documents could leave an organization the victim of a ransomware attack and having to defend its decision not to implement the White House and CISA recommendations.
