CAPLAW enews brief

White House Urges Action Against Ransomware Attacks

By CAPLAW Staff
June 2021

Responding to growing cybersecurity concerns arising from recent, high-profile ransomware attacks, on June 8, 2021 the White House released a memo, "What We Urge You To Do To Protect Against The Threat of Ransomware". The memo urges businesses to implement several strategies and practices that can protect their data and other private organizational information against ransomware and other cyberattacks.

Guidance from the President's "Improving the Nation's Cybersecurity" Executive Order

The memo references several key components from a May 2021 Executive Order that outlined the Biden Administration's plan to protect the federal government from future cyberattacks, recommending that private individuals and entities also incorporate these measures into their cybersecurity policies and practices. These measures include implementing:

- Multifactor authentication to reduce the chances of a password being compromised;
- Endpoint detection and response to identify malicious activity and block it;
- Encryption to protect data from misappropriation; and
- A skilled and empowered cybersecurity team to identify and prevent security threats.

Data Backups

The memo recommends frequently backing up organizational data, system images, and configurations to offline locations not connected to the business network. Creating and regularly testing these backups can protect your organization's data and/or systems from being irretrievably encrypted or stolen by providing a reliable backup to restore from.

System Updates and Patches

The memo urges organizations to regularly update and patch operating systems, applications, and firmware, suggesting the use of a centralized patch management system to help stay on top of updates for their systems. Consistently implementing system updates helps to keep your organization one step ahead of hackers looking for software vulnerabilities to exploit.

Response Plan Testing

The memo strongly recommends frequently testing security systems to find gaps and vulnerabilities. Some questions to keep in mind as these tests are conducted include: Are you able to sustain business operations without access to certain systems? For how long? Would you turn off all operations if other systems such as billing were offline?

Third Party Consultants

While the memo suggests hiring an in-house security team wherever possible, a fresh set of eyes can sometimes find problems and vulnerabilities that an in-house team may overlook. For that reason, the memo also recommends using a third-party security expert to test your organization's security systems and their ability to respond to a sophisticated cyberattack.

Network Segmenting

While many past ransomware attacks primarily focused on stealing data, hackers are increasingly turning their attention toward disrupting organization operations instead. Consequently, the memo recommends segmenting internet connection sharing (ICS) networks such that compromised networks can be manually isolated in the event of a ransomware attack. Doing this can reduce a ransomware attack's impact on organizational operations and minimize its access to critical data and functions. Organizations should also regularly test their manual network controls to ensure that safety-critical functions can remain accessible and usable during a cyberattack.

For more information on cybersecurity and data protection, please refer to this installment of CAPLAW's "Conversations With Experts" series.

This publication is part of the Community Services Block Grant (CSBG) Legal Training and Technical Assistance (T/TA) Center. It was created by Community Action Program Legal Services, Inc. (CAPLAW) in the performance of the U.S. Department of Health and Human Services, Administration for Children and Families, Office of Community Services Cooperative Agreement – Grant Award Number 90ET0482-01. Any opinion, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of HHS and ACF. The contents of this publication are intended to convey general information only and do not constitute legal advice. Any communication through this publication or through CAPLAW's website does not constitute or create an attorney-client relationship. If you need legal advice, please contact CAPLAW or another attorney directly.