THREAT BULLETINS

White House Memo to Protect Against The Threat of Ransomware

TLP:WHITE

Jun 03, 2021

The following text comes from the attached document from Anne Neuberger, the Deputy Assistant to US President Joseph Biden, and Deputy National Security Advisor for Cyber and Emerging Technology:

The number and size of ransomware incidents have increased significantly, and strengthening our nation's resilience from cyber attacks, both private and public sector, is a top priority of the President's. Under President Biden's leadership, the Federal Government is stepping up to do its' part, working with like-minded partners around the world to disrupt and deter ransomware actors. These efforts include disrupting ransomware networks, working with

international partners to hold countries that harbor ransomware actors accountable, developing cohesive and consistent policies towards ransom payments and enabling rapid tracing and interdiction of virtual currency proceeds.The private sector also has a critical responsibility to protect against these threats. All organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location. But there are immediate steps you can take to protect yourself, as well as your customers and the broader economy. Much as our homes have locks and alarm systems and our office buildings have guards and security to meet the threat of theft, we urge you to take ransomware crime seriously and ensure your corporate cyber defenses match the threat. The most important takeaway from the recent spate of ransomware attacks on US, Irish, German and other organizations around the world is that companies that view ransomware as a threat to their core business operations rather than a simple risk of data theft will react and recover more effectively. To understand your risk, business executives should immediately convene their leadership teams to discuss the ransomware threat and review corporate security posture and business continuity plans to ensure you have the ability to continue or quickly restore operations.

Below you will find the U.S. Government's recommended best practices; we've selected a small number of highly impactful steps to help you focus and make rapid progress on driving down risk.

- **Implement the five best practices from the President's Executive Order:** President Biden's Improving the Nation's Cybersecurity Executive Order is being implemented with speed and urgency across the Federal Government. We're leading by example because these five best practices are high impact: multi-factor authentication (because passwords alone are routinely compromised), endpoint detection& response (to hunt for malicious activity on a network and block it), encryption (so if data is stolen, itis unusable) and a skilled, empowered security team (to patch rapidly, and share and incorporate threat information in your defenses). These practices will significantly reduce the risk of a successful cyber-attack.
- **Backup your data, system images, and configurations, regularly test them, and keep the backups offline:** Ensure that backups are regularly tested and that they are not connected to the business network, as many ransomware variants try to find and encrypt or delete accessible backups. Maintaining current backups offline is critical because if your

network data is encrypted with ransomware, your organization can restore systems.

- **Update and patch systems promptly:** This includes maintaining the security of operating systems, applications, and firmware, in a timely manner. Consider using a centralized patch management system; use a risk-based assessment strategy to drive your patch management program.
- **Test your incident response plan:** There's nothing that shows the gaps in plans more than testing them. Run through some core questions and use those to build an incident response plan: Are you able to sustain business operations without access to certain systems? For how long? Would you turn off your manufacturing operations if business systems such as billing were offline?
- **Check Your Security Team's Work:** Use 3rd party pen testers to test the security of your systems and your ability to defend against a sophisticated attack. Many ransomware criminals are aggressive and sophisticated and will find the equivalent of unlocked doors.
- **Segment your networks:** There's been a recent shift in ransomware attacks –from stealing data to disrupting operations. It's critically important that your corporate business functions and manufacturing/production operations are separated and that you carefully filter and limit internet access to operational networks, identify links between these networks and develop workarounds or manual controls to ensure ICS networks can be isolated and continue operating if your corporate network is compromised. Regularly test contingency plans such as manual controls so that safety critical functions can be maintained during a cyber incident.

Ransomware attacks have disrupted organizations around the world, from hospitals across Ireland, Germany, and France, to pipelines in the United States and banks in the U.K. The threats are serious, and they are increasing. We urge you to take these critical steps to protect your organizations and the American public. The U.S. Government is working with countries around the world to hold ransomware actors and the countries who harbor them accountable, but we cannot fight the threat posed by ransomware alone. The private sector has a distinct and key responsibility. The federal government stands ready to help you implement these best practices.

Alert ID 6aad0947

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Tags White House

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more update and alerts, visit: **https://health-isac.cyware.com**