Are You Complying with the Executive Order on Cybersecurity?

Author: Jim Shook, Director, Compliance Practice, Global Technology Office, Dell EMC Federal

In May 2017, the President issued an Executive Order on Cybersecurity. Among other requirements, the order holds agency heads accountable for appropriate cyber defenses:

"Agency heads will be held accountable by the President for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data."

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11, 2017. The order also mandates the use of the NIST Cybersecurity Framework (https://www.nist.gov/cyberframework) in managing cybersecurity risk.

The Threats

Is your agency complying with the order? Over the last few years, cybersecurity threats have evolved from traditional data theft into data destruction and ransomware attacks. These newer threats are vastly different because they directly impact and threaten the operation of IT infrastructures.

Ransomware itself has grown into a significant threat. Originally, ransomware might attack and encrypt a single endpoint, such as a desktop. To expand their reach, criminals quickly added capabilities to encrypt not just the host, but other devices and shares that could be accessed from the host; and then started moving laterally to other devices before starting the encryption process. These new capabilities threatened not only production servers and data, but also the backup infrastructure.

A Risk-Adjusted Approach

These new threats are precisely the type of attacks contemplated by the classic evaluation approach required in the order: assessing both the risk (probability) and magnitude (scope of harm) for threats.

The risk of a ransomware or destructive attack is high – 60 percent of organizations were hit by ransomware in 2016. By mid-2017, more than half of organizations had been hit by a ransomware attack at least twice (Druva Ransomware Report 2017).

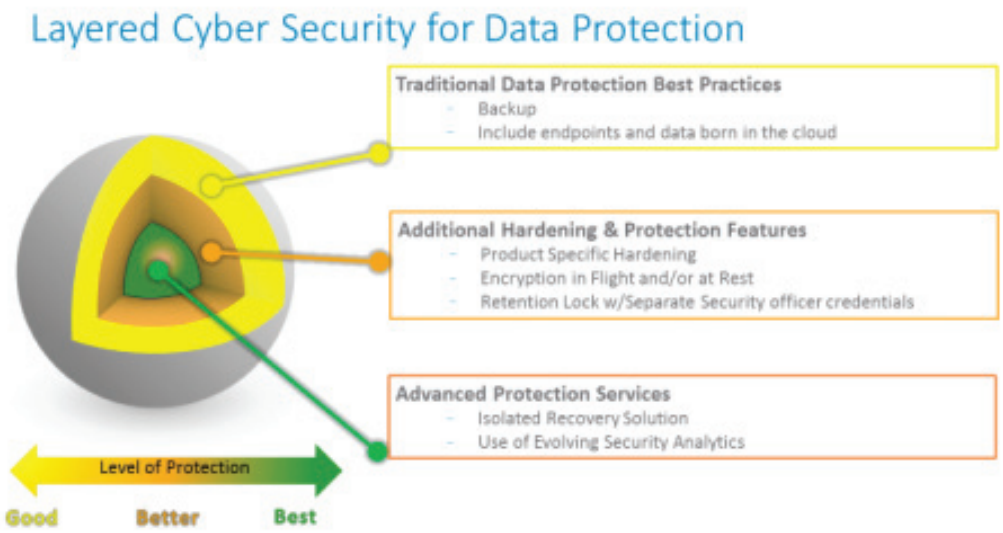
The magnitude of harm from a ransomware or destructive attack can also be significant. In 2016, a utility in the Midwest spent about $2.5M recovering from a single attack, and a healthcare organization estimated its losses and recovery costs at $10M. In the for-profit space, several organizations reported losses of over $200M from the NotPetya attacks of June 2017.

What Should You Do?

The high risk and magnitude of ransomware and destructive threats means that agencies must address this problem under requirements of the order.

Many experts, including several who work for federal agencies, recommend a backup as the best defense to a ransomware attack. So while a layered defense including employee training, anti-malware and other defenses are important, the specific response to a ransomware threat requires a "recover" strategy as outlined in NIST's Cybersecurity Framework.

The backup strategy itself can be tailored to match the value of the data. We recommend protecting data for cybersecurity recovery at different levels, based upon its criticality. Three levels of protection – in increasing levels of security – can be deployed:



- Standard backup – including a backup for data stored in the cloud;
- Backup stored on a hardened backup infrastructure – deploying least privilege, network segmentation, securing CIFS / NFS shares (or better yet, using a different protocol such as Boost), deploying retention lock / WORM capabilities, etc.; or
- An isolated backup protected with an operational, logical "air gap." This backup infrastructure is minimally exposed to the outside world and ready for quick restores (unlike a tape backup which is undependable and can have a very long recovery time).

Conclusion

Cyber defenses should match the threats that we are all seeing today. Make sure that your infrastructure is protected from ransomware and destructive attacks with appropriate defenses.

Dell EMC recommends Data Protection Backup and Isolated Recovery for efficient, cost effective backup and recovery.

Learn more, here:

Data Protection Backup: https://www.dellemc.com/en-us/data-protection/index.htm

Isolated Recovery: https://www.dellemc.com/en-us/solutions/data-protection/isolated-recovery-solution.htm