The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

ICI VIEWPOINTS

May 26, 2017

Cybersecurity at Work: I Know What You Know!

Part of a series of ICI Viewpoints *covering cybersecurity issues.*

In the previous installment of this series I mentioned that this post would address steps that you should take if your computer is hacked. Well, in light of the WannaCry/WannaCrypt ransomware outbreak, it seems appropriate to address not only what to do, but how to think about the threats facing us.

Because many malware strains are delivered via phishing exploits, the standard training emphasizes caution—don't open an email from someone you don't know, for example, or an email you were not expecting. We need to start thinking more critically about threats and the attackers. We need to go further. Does an email from a trusted source make sense when examined closely (consider the recent Google Docs phishing example)? What does Microsoft's Patch Tuesday lead to? And what does that threat intelligence and analysis report really tell you?

It should be obvious to everyone that, in part, the reason these exploits are successful is because the attackers know your technology. They buy the same firewall, anti-virus, data loss prevention, and other software that you do—so they can devise ways to exploit them. The Google Docs phish did not use malware but tricked the recipient of an email into granting permissions to a third-party application. After telling you that you were added to a Google Doc, and asking you to click through to the site, you were taken to a legitimate account screen with a list of logged-into Google accounts. Once there, you then selected the account that would enable you to view the document—where "Google Docs" is waiting, and asks for permission or privileges to access the account. Permission? Why does Google need privileges to access an account it can already access? That answer is, it doesn't. And that is where critical thinking comes into play.

Similarly, Microsoft's "Patch Tuesday"—when the firm releases security patches for its software products—has been a formally scheduled event since 2003. Guess what Wednesday is? Exploit Day! There is no question that the patches are helpful, but attackers know that many firms are on a 60-day patch cycle. When Patch Tuesday arrives, the bell has rung and it's time for attackers to begin taking advantage of the vulnerabilities that Microsoft has just highlighted. The attackers know that patching is not easy, and that some firms will experience issues and delays. We need to realize that communications about events and services like Patch Tuesday go to the bad guys as well as to us.

Threat intelligence also presents challenges. There are many fee-based subscription

services that provide threat intelligence, and there are countless free reports with analysis on the latest exploit. Undoubtedly, such threat intelligence can provide real value—for example, it might provide the early warning and information—and, thus, the lead time—you need to prevent a successful attack. But guess who also subscribes to these services and reports? Let's not delude ourselves into thinking that we are receiving a secret piece of intelligence. A report that provides analysis on a particular attack tips off the attacker that it has been discovered and gives them time to modify the attack. We need to keep this in mind.

So where does this leave us? Awareness training on phishing, for example, is not enough. We must put ourselves in the mindset of the attacker. Employees should think about their firm's data in terms of what an attacker might want to monetize, who has access to it, and which people present an interesting target.

The WannaCry/WannaCrypt attack should make everyone examine their emergency-response procedures, including whether the topic of making a ransom payment has been contemplated. Whether a firm decides to pay a ransom or not, a good place to first check for decryption tools is No More Ransom. In addition, here are some tips for preventing ransomware.

The next post in this series will explain the benefits of a principles-based approach to standards-setting.

Additional Resources:

Information Security Resource Center

Other Posts in This Series:

- Cybersecurity at Work: Creating Passwords That Are More Secure
- Cybersecurity at Work: Incident Response Plans and What They Entail
- Cybersecurity at Work: Exercise Is Important
- Cybersecurity at Work: The Benefits of Information Sharing Networks
- Cybersecurity at Work: The Risks of Information Sharing
- Cybersecurity at Work: Keeping Secure When Away from the Office
- Cybersecurity at Work: I Know What You Know!
- Cybersecurity at Work: To Confront Evolving Threats, Flexibility Is Key