Preliminary Cybersecurity Framework Comments

Orlie Yaniv Fri, Dec 13, 2013 at 4:37 PM

FireEye applauds NIST and industry for development of the Preliminary Cybersecurity Framework. We agree that protecting our Nation's critical infrastructure requires the development and execution of sound risk management practices that allow organizations to reach evolving levels of maturity over time. This structure will provide critical infrastructure companies with a useful baseline from which to develop and improve their cybersecurity programs.

However, as detailed with specificity in the attached comment matrix, the Framework does not sufficiently mitigate risk from advanced cyber threats that utilize never seen before malware or exploit previously unknown exploits (zero-day attacks). According to the December 2013 Ponemon Institute Report on *The State of Advanced Persistent Threats*, 68% of respondents to a recent survey of IT and IT security practitioners indicated that zero-day attacks are their organization's greatest threat. 72% say exploits and malware have evaded their intrusion detection systems (IDS) and 76% say they have evaded their AV solutions. Clearly, attacks that are designed to evade traditional countermeasures such as firewalls, intrusions and IDS/IPS are an inherent and escalating component of our Nation's threat landscape and must be addressed. By omitting references to emerging controls and best practices such as NIST *Special Publication 800.53 Rev4, Security and Privacy Controls for Federal Information Systems and Organizations, Security Control 44 Detonation Chambers* (Security Control 44) that help mitigate risk from advanced attacks, the Framework does not recognize or reference the advancing state of these attacks, which is an oversight that will undermine our national and economic security. It is critical that NIST exercise leadership by recognizing and documenting the accelerating nature of the threat and ways to mitigate attendant risk in this version of the Framework.

Accordingly, we recommend that the Final Version of the Framework:

(1) incorporate Security Control 44 as an informative reference for a number of subcategories in Appendix A; and

(2) include the Mitigating Risk From Advanced Cyber Threats an "Area for Improvement" in Appendix C.

Details, including proposed language for these recommendations, can be found in the attached spreadsheet.

These recommendations are driven in part by FireEye's concern that adoption of the current Framework Core may in practice evolve into a compliance activity for some companies. While FireEye recognizes that the intent of the Framework is to encourage critical infrastructure to "…add Subcategories and Informative References that are relevant to them and enable them to more effectively manage their cybersecurity risk," the level of effort associated with development of tailored profiles may be too great for some companies and they may just adopt safeguards and activities in Framework Core as a compliance function. Without specific references to controls that offset the full range of threats and risks critical infrastructure companies face today, FireEye is concerned that overall levels of risk will remain high in those organizations. As an example, the California Public Utilities Commission (CPUC) released a policy paper on September 19, 2012 entitled "Cybersecurity and the Evolving Role of State Regulation: How it Impacts the California Public Utilities Commission." The paper states that "Compliance is an important component of addressing cybersecurity, but it is not enough to ensure that the rapidly evolving risks are adequately considered and acted upon effectively." This CPUC publication is a great example of how some state lawmakers are lobbying for change to protect critical infrastructure from advanced cybersecurity attacks.

In addition, FireEye recommends that future iterations of the Framework:

· Provide an accelerating set of guidance profiles by implementation tier. The current version of the Framework only provides guidance for common activities and does not map that guidance to a target maturity level. Providing such mapping guidance will enable organizations to more easily understand how to the achieve the desired end state of cybersecurity.

- Provide more guidance on appropriate risk management at each implementation tier. For example, more mature organizations measure risk more quantitatively, understand their model and variables for measuring risk, use industry specific threat data based on a well-defined asset base, measure risk more frequently and have metrics defined with a history to demonstrate the effectiveness of their risk management programs.

- Expand the guidance related to secure engineering practices. Secure engineering practices reduce the number and severity of vulnerabilities in deployed technology that can be exploited by an advanced threat, establish processes to ensure maintenance and response, and improve system resiliency.

Please do not hesitate to contact me with any questions or requests for clarification.

Sincerely,

Orlie

Orlie Yaniv
Director, Government Affairs and Policy

Next Generation Threat Protection

FireEye Comments Preliminary Cybersecurity Framework 12-13-2013 final.xls
31K