TECH BRIEF

Hacking critical infrastructure: Keeping our nation safe

ENJOY SAFER TECHNOLOGY™

HACKING CRITICAL INFRASTRUCTURE: KEEPING OUR NATION SAFE

By Cameron Camp, ESET Security Researcher

When a computer is hacked, data is compromised. If the nation's power grid or other critical system is hacked, it could set off a disaster. Scenarios such as penetrating a hydroelectric dam's control systems and flooding whole valleys by using rogue malware might make for scary movie plots, but the threat is not farfetched at all.

Making sure our nation's critical infrastructure could withstand a cyber-assault is a top priority for the federal government. The National Institute of Standards and Technology (NIST) has collaborated with thousands of individuals and organizations from industry, academia and government to develop a set of guidelines, best practices and standards to address cybersecurity risks. The effort culminated in the release of the Framework for Improving Critical Infrastructure Cybersecurity.

A voluntary standard

The framework was developed in response to an Executive Order to create voluntary cybersecurity standards, after efforts for cybersecurity laws stalled in Congress. The term "voluntary framework" underscores that the document is not intended to be the basis for a future set of mandatory standards. It is, however, expected to be a first step in a continuous process to improve the nation's cybersecurity.

The effort that went into creating the framework included a massive amount of input from the private sector through written input as well as a series of workshops around the country. Each workshop was attended by hundreds of people, including representatives of organizations such as utilities and transportation companies that maintain critical infrastructure.

While voluntary, the framework is having an impact. Many companies are already adopting its guidelines involving prevention, detection, preparation and recovery planning. There has also been talk of cyber-risk insurance providers using the framework as a benchmark for underwriting; companies that demonstrate conformance could potentially purchase cyber-insurance at lower rates.

Elements of the cybersecurity framework

The framework was built to assess firms' security and bring them up to a safer level. It applies basic cybersecurity standards by placing them in the context of business risk and can be used by organizations regardless of size.

There are multiple dimensions to a cybersecurity initiative. Within a smaller organization especially, the first question is usually "What specific steps or actions should we take?" However, those answers vary greatly from organization to organization. The framework, therefore, is not strictly a set of sequential actions or steps but a resource that allows an organization to take a methodological approach to a multidimensional effort and determine the actions that are most appropriate given the risks and resources.

Here are the major elements of the framework:

The framework core organizes cybersecurity-related actions and desired outcomes into an approachable hierarchy. Since published standards, guidelines and practices are already available from sources

such as COBIT, ISA, ISO/IEC and NIST, the framework document doesn't reiterate them but rather provides references to them. The Framework Core provides organization and structure, grouping actions and practices into categories and subcategories, with the broadest being the functional areas of Identify, Protect, Detect, Respond and Recover. This well-structured hierarchy provides a basis for understanding cybersecurity within an organizational context and communicating about it with executives and stakeholders.

Framework implementation tiers help an organization understand and characterize its cybersecurity practices and risk processes. There are four defined tiers, termed Partial, Risk-Informed, Repeatable and Adaptive, and they reflect a progression from an ad hoc, reactive approach to one in which cybersecurity risk management is fully informed by business needs, integrated into overall risk management, and continuously monitored and improved. The tiers are not necessarily target states, and the highest tiers are not appropriate for all organizations. Movement to a higher tier is appropriate when a change would reduce cybersecurity risk and be cost effective.

Framework profiles are the "action" element and are specific to each organization. To develop a profile, the organization draws from the outcomes and activities defined in the Framework Core that present the best or most important opportunities for improving cybersecurity based on business drivers and risk assessment. By describing the current state through a Current Profile and desired state through a Target Profile and then comparing the two, the organization is able to create a roadmap for improving cybersecurity. Assessing the cost of addressing each of the identified gaps allows the organization to prioritize and implement improvements cost effectively.

The NIST document includes several other important sections that deal with practical application of the framework:

- **Recommendations on coordinating framework implementation within an organization**
- **Sample approaches for applying the framework**
- **Recommendations for communicating about cybersecurity with stakeholders**
- **A methodology for protecting individual privacy and civil liberties; this was required by the Executive Order that prescribed the development of the framework**

The framework is an important first step in addressing risks that have strategic national-security implications. It complements any risk management or cybersecurity processes and programs that are already in place and can serve as a reference for establishing cybersecurity programs for organizations that need one.

Employees of ESET North America played key roles in developing the framework, including submitting comments in the very early stages to help drive the process and participating in the workshops.

For more information on protecting your mobile devices for both business and home, visit eset.com/us.