Security guidelines in action

Organizations often face an overwhelming amount of risk. Developing a security plan from the beginning that addresses all risk can be challenging. This makes security frameworks a useful option.

Previously, you learned about the NIST Cybersecurity Framework (CSF). A major benefit of the CSF is that it's flexible and can be applied to any industry. In this reading, you'll explore how the NIST CSF can be implemented.

> The NIST CSFs five functions: identify, protect, detect, respond, and recover.

Origins of the framework

Originally released in 2014, NIST developed the Cybersecurity Framework to protect critical infrastructure in the United States. NIST was selected to develop the CSF because they are an unbiased source of scientific data and practices. NIST eventually adapted the CSF to fit the needs of businesses in the public and private sector. Their goal was to make the framework more flexible, making it easier to adopt for small businesses or anyone else that might lack the resources to develop their own security plans.

Components of the CSF

As you might recall, the framework consists of three main components: the *core*, *tiers*, and *profiles*. In the following sections, you'll learn more about each of these CSF components.

Core

The CSF core is a set of desired cybersecurity outcomes that help organizations customize their security plan. It consists of five functions, or parts: Identify, Protect, Detect, Respond, and Recover. These functions are commonly used as an informative reference to help organizations *identify* their most important assets and *protect* those assets with appropriate safeguards. The CSF core is also used to understand ways to *detect* attacks and develop *response* and *recovery* plans should an attack happen.

Tiers

The CSF tiers are a way of measuring the sophistication of an organization's cybersecurity program. CSF tiers are measured on a scale of 1 to 4. Tier 1 is the lowest score, indicating that a limited set of security controls have been implemented. Overall, CSF tiers are used to assess an organization's security posture and identify areas for improvement.

Profiles

The CSF profiles are pre-made templates of the NIST CSF that are developed by a team of industry experts. CSF profiles are tailored to address the specific risks of an organization or industry. They are used to help organizations develop a baseline for their cybersecurity plans, or as a way of comparing their current cybersecurity posture to a specific industry standard.

Note: The core, tiers, and profiles were each designed to help any business improve their security operations. Although there are only three components, the entire framework consists of a complex system of subcategories and processes.

Implementing the CSF

As you might recall, compliance is an important concept in security. **Compliance** is the process of adhering to internal standards and external regulations. In other words, compliance is a way of measuring how well an organization is protecting their assets. The **NIST Cybersecurity Framework (CSF)** is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. Organizations may choose to use the CSF to achieve compliance with a variety of regulations.

Note: Regulations are rules that *must* be followed, while frameworks are resources you can *choose* to use.

Since its creation, many businesses have used the NIST CSF. However, CSF can be a challenge to implement due to its high level of detail. It can also be tough to find where the framework fits in. For example, some businesses have established security plans, making it unclear how CSF can benefit them. Alternatively, some businesses might be in the early stages of building their plans and need a place to start.

In any scenario, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) provides detailed guidance that any organization can use to implement the CSF. This is a quick overview and summary of their recommendations:

- **Create a current profile** of the security operations and outline the specific needs of your business.
- **Perform a risk assessment** to identify which of your current operations are meeting business and regulatory standards.
- **Analyze and prioritize existing gaps** in security operations that place the businesses assets at risk.
- **Implement a plan of action** to achieve your organization’s goals and objectives.

Pro tip: Always consider current risk, threat, and vulnerability trends when using the NIST CSF.

You can learn more about implementing the CSF in this report by CISA that outlines how the framework was applied in the commercial facilities sector

.

Industries embracing the CSF

The NIST CSF has continued to evolve since its introduction in 2014. Its design is influenced by the standards and best practices of some of the largest companies in the world.

A benefit of the framework is that it aligns with the security practices of many organizations across the global economy. It also helps with regulatory compliance that might be shared by business partners.

Key takeaways

The NIST CSF is a flexible resource that organizations may choose to use to assess and improve their security posture. It's a useful framework that combines the security best practices of industries around the world. Implementing the CSF can be a challenge for any organization. The CSF can help business meet regulatory compliance requirements to avoid financial and reputational risks.

Revision #1
Created 17 July 2023 03:10:48 by naruzkurai
Updated 15 August 2023 18:44:10 by naruzkurai