CERT PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Inside Defense-in-Depth

Key Message: Defense-in-Depth is one path toward enterprise resilience — the ability to withstand threats and failures. The foundational aspects of compliance management and risk management serve as stepping-stones to and supports for other, more technical aspects.

Executive Summary

The concept of Defense-in-Depth historically has been somewhat vague, referring to many different security mechanisms all working in tandem to reduce risk. But how do you measure your level of Defense-in-Depth? How do you establish a baseline, formulate an implementation plan, and monitor your performance?

In this podcast, Kristopher Rush, co-author of CERT's Defense-in-Depth curriculum, explains a layered approach to this concept that allows organizations to approach Defense-in-Depth via a clear framework.

PART 1: DEFINING DEFENSE-IN-DEPTH; GETTING STARTED

Background

Defense-in-Depth involves multiple, related controls addressing different security concerns across an organization. It is a layered approach.

Think in terms of "information insurance." If one layer fails, other layers are still in place to sustain your network despite attacks and failures.

Defense-in-Depth Structure

We view Defense-in-Depth in terms of eight different conceptual containers:

- Compliance Management
- Risk Management
- Identity Management
- Authorization Management
- Accountability Management
- Availability Management
- Configuration Management
- Incident Management

With this framework, you can look at each container individually, determine what you have, and decide whether or not you need to devote more resources to that container.

Best approach: Ingrain Defense-in-Depth into your organizational culture.

DON'T hand it to one person and hope they manage to achieve Defense-in-Depth for the organization on their own.

Where to Start?

It all starts with compliance management. You can't really implement security unless you have a **reason** for having security.

Important goals:

- Support the business mission.
- Provide continuity of business in the face of threats and failures.

Define your policy so you know what resources you need to secure and what you're seeking to achieve. Policy should be general enough that it won't need to change much over time.

Second, engage in risk management:

- Identify your critical assets.
- Determine the potential loss to your organization if those assets become unavailable.
- Examine threats to those assets.
- Rank the assets' importance.
- Determine general security requirements for the assets.

Risk management and compliance management serve as foundations for all of the other components of Defense-in-Depth.

PART 2: OBTAINING BUY-IN

Who's in Charge?

Depending on your organization, various people may be in charge of the Defense-in-Depth effort. The point person may be a CIO or CISO — which is often optimal — but also might be a lower-level person.

However, keep in mind that Defense-in-Depth requires full organizational buy-in! The Defense-in-Depth leader must have the clout to accomplish this.

Achieving Buy-In

There are different ways to achieve buy-in:

- External regulatory forces (for example, Sarbanes-Oxley) can force buy-in by default.
- Engaging in continual user education can keep Defense-in-Depth top-of-mind.

PART 3: A CONTINUOUS PROCESS

Gauging Progress

How do you determine when you've achieved Defense-in-Depth?

- How much security is enough?
- Do I have it?
- Am I secure?

There is no clear-cut answer. Security is not "fix it and forget it."

Defense-in-Depth requires an ongoing commitment, including maintenance and monitoring of infrastructure.

Maintenance and Monitoring

Ask yourself:

- Have you followed and implemented the Defense-in-Depth framework as best you can with the resources you have?
- Given the mechanisms you have in place, do you think you've achieved the level of risk management required for your assets?
- Look to accountability management: Does the security you envision match what you're seeing in your access and traffic logs?

Yes, this requires a lot of legwork!

Roles of the Defense-in-Depth Curriculum

A Defense-in-Depth curriculum is available on the CERT website at http://www.cert.org/archive/pdf/Defense_in_Depth092106.pdf.

It plays different roles for different audiences:

- Managers — a good starting point to reach back into the technical field and become familiar with concepts for achieving information assurance.
- System administrators — a good way to become familiar with how managerial and policy concepts tie into technology.

Future Direction

Defense-in-Depth is designed as a moldable, expandable framework. It can remain relevant as technologies and implementations change because it is not based on specific technologies or implementations. Likewise, even as the regulatory framework changes, along with the environment in which companies operate, general principles within the curriculum are designed to be relatively timeless.

Resources

May, Christopher J.; Hammerstein, Josh; Mattson, Jeff; Rush, Kristopher. Defense-in-Depth: Foundations for Secure and Resilient IT Enterprises, CERT Program, Carnegie Mellon University, September 2006.
