Rapid7 Overview

Introduction

Attackers are constantly probing Networks, Systems, and Web applications in search of exploitable vulnerabilities and organizations failing to test and secure their Internet facing information assets often fall victim.

These probes and attacks are not limited to the size or sophistication of an organization rather its security posture.

A vulnerability assessment is an important part of an effective countermeasure and the benefits are to:

- Identify threats facing an organization's information assets so they can be quantified to produce a risk analysis.
- Provide an organization with assurances that they have a thorough and comprehensive assessment of their organizational security policies.
- Gain and maintain certification to industry regulations (PCI, Sarbanes-Oxley, HIPAA, etc).
- Adopt best practice by conforming to legal and industry regulations.

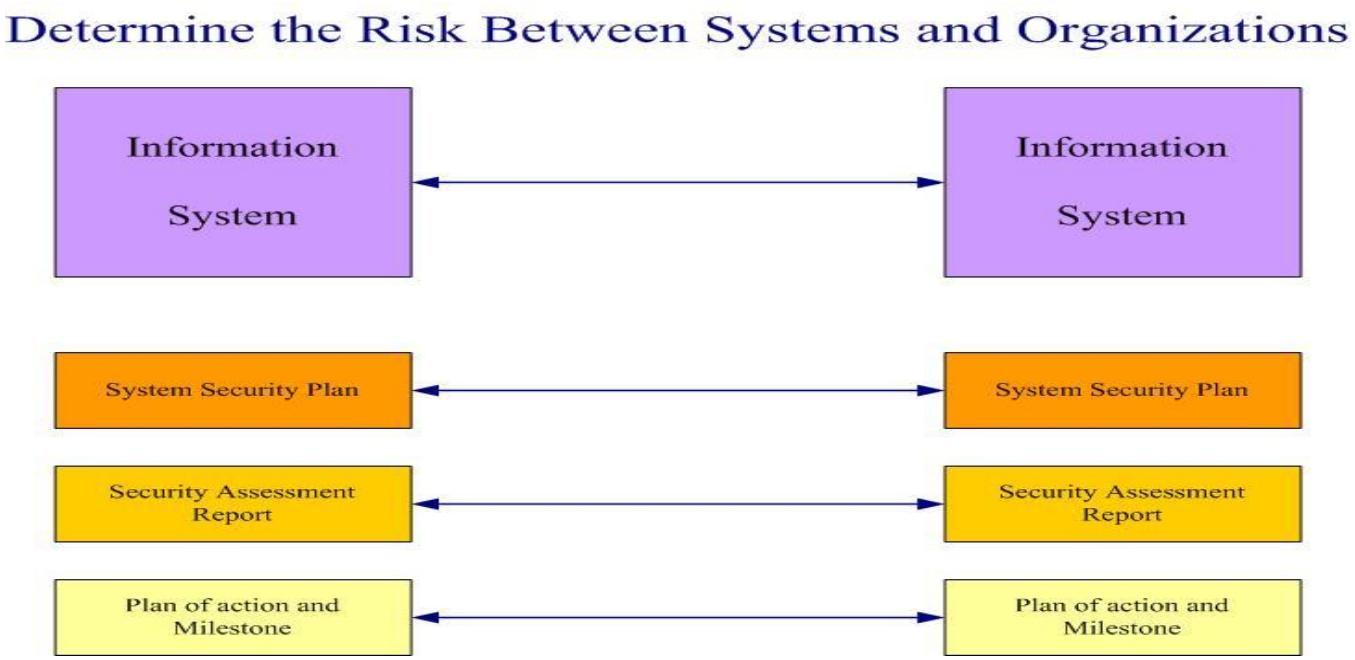
Overview

These assessments will benefit any organization that seeks to verify implemented security controls, suspects their IT infrastructure may have been compromised, desires to eliminate security weaknesses and protect their information technology infrastructure before a compromise occurs, or simply wants to establish a security baseline.

Ultimately a successful compromise could cost thousands and possibly millions of dollars in losses to reputation, customer confidence, market share, productivity, legal recourse, and more. We provide you with the information necessary to make well-informed decisions on the balance between usability and security.

The objective of performing required security risk assessments is to enable Corporate to accomplish its mission of securing systems that capture, process, transmit and store company and information.

This enables management to make well-informed decisions regarding company risk; help justify IT and security expenditures, and assist management in authorizing systems.



Description

A risk assessment is the process of identifying and quantifying threats and vulnerabilities of information systems or applications and evaluating alternatives for mitigating or accepting the resulting appropriate judgments about system controls and risks. A risk assessment should be performed:

1) Throughout a corporate life cycle, and should occur when threats change / increase;

2) At periodic intervals established by the corporate commensurate with the sensitivity of the data;

3) Prior to the approval of design specifications for new systems or applications (dev / test);

4) Whenever a significant change occurs to the systems (i.e., adding local area networks, adding VLANs, VPNs, dial-up connectivity, etc…);

5) To determine the need and type of approved protection technique for the systems again corporate and changing regulatory compliance

The Rapid7 Scanner can perform scheduled and on demand Internal and External Vulnerability Scans selectively probing and interrogating the perimeter and interior routers and firewalls, communication services, operating systems, applications to uncover and report systems vulnerabilities that might be open to attack. Rapid7's vulnerability assessment service provides a valuable baseline for determining appropriate safeguards.

Internal vs. External Vulnerability Scan

There are two types of vulnerability scans that provide you with contrasting perspectives of your network infrastructure - Internal and External.

- **An External vulnerability** scans is conducted with known External Corporate Netblocks of the target environment and is performed from the Internet outside of the network perimeter. The External scan tests Internet - DNS, Router, Firewall IP addresses, websites and email systems. After the initial stage, scanning techniques are utilized in order to assess which systems are vulnerable to outside access, similar to the process a potential attacker might use.

- **An Internal vulnerability** scan is conducted against Corporate's internal network based on given internal Netblock infrastructure. Due to the fact that the scan is initiated from inside the firewalls, additional system and network information will be accessible. The Internal scan focuses on system configurations and security policies. In the event an attacker compromises a single system, you would want to contain the attack to avoid further penetration of your infrastructure. The vulnerabilities discovered by an internal scan will help you to be proactive and update your systems in order to solidify your security posture.

Managed Vulnerability Scan

The Rapid7 Vulnerability Scanning service will maintain an effective security posture by keeping up to date on recent vulnerabilities, changes in your infrastructure and the identification of any new security weaknesses. Rapid7 methodology for conducting the Vulnerability Scan is done in three (3) phases:

1) **Discovery baseline**
   The scans are also performed from two venues the first from the Internet to determine vulnerability from outside the state network, and second from the Internal network backbone, to determine vulnerability from other departmental and inter-networks

2) Scanning / Craft vulnerability tests
   Calculate the probability of compromise of a vulnerable host on the target networks

3) Analysis / Review / Remediation