INCIDENT RESPONSE PROCESS

Introduction

Incident response is an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. An incident response plan includes a policy that defines, in specific terms, what constitutes an incident and provides a step-by-step process that should be followed when an incident occurs.

According to the Relitrade, there are six steps to handling an incident most effectively:

Preparation:

Relitrade educates users and IT staff of the importance of updated security measures and trains them to respond to computer and network security incidents quickly and correctly.

Identification:

Relitrade IT team activated to decide whether a particular event is a security incident. The team may contact the concern vendors, which tracks Internet security activity and has the most current information on viruses and worms.

Containment:

The team determines how far the problem has spread and contains the problem by disconnecting all affected systems and devices to prevent further damage.

Eradication:

The team investigates to discover the origin of the incident. The root cause of the problem and all traces of malicious code are removed.

Recovery:

Data and software are restored from clean backup files, ensuring that no vulnerabilities remain. Systems are monitored for any sign of weakness or recurrence.

Lessons learned:

The team analyses the incident and how it was handled, making recommendations for better future response and for preventing a recurrence.