SANS Forensic/IR Summit
Strategy Panel

Bret Padres
Director, Digital Forensics

October 14, 2008
Overview

• How do you answer the following questions from clients after confirming an incident has occurred:
  • What type of data loss should we be more concerned with PII or PCI?
  • What should our first priority be? Detailed descriptions of the data that was stolen OR a detailed description of how the break in occurred?
  • If we hire an outside firm to help us with IR: What are the 3 questions that we should ask?
Overview

• Based on recent case studies, what is the number one vector of entry leading to the compromise of an organization's network and or data?

• What are some recommended security policies every organization should adhere by in order to prevent future attacks and outbreaks?
Ugly Baby
Ugly Baby

Cyber Speak

TURNING INFORMATION INTO INTELLIGENCE
After Confirmation of an Incident

• What type of data loss should we be more concerned with PII or PCI?
  • The wrong question to be asking at this time. Investigation focus should be on determination of **scope**:
    • Identification of indicators of compromise.
    • Development of indicator detection mechanisms.
  • Effort to classify data at risk can begin in parallel.
After Confirmation of an Incident

• What should our first priority be? Detailed descriptions of the data that was stolen OR a detailed description of how the break in occurred?

• Eventually you will have to do both.
• Without knowing how the break in occurred, you will not be sure of scope of data loss.
• As data is deemed to be at risk of loss, a parallel effort to classify that data should be undertaken.
After Confirmation of an Incident

• If we hire an outside firm to help us with IR: What are the 3 questions that we should ask?
  
  • What is Stroz Friedberg’s phone number?
  • How do we get a hold of someone at Stroz Friedberg?
  • What is the email address of that guy from Stroz Friedberg?
After Confirmation of an Incident

- If we hire an outside firm to help us with IR: What are the 3 questions that we should ask?
  - Ask them to explain their IR methodology.
  - Ask about their ability to scale.
  - Ask for BIOs and CVs of the responders.
Based on Recent Case Studies

• What is the **number one vector** of entry leading to the compromise of an organization's network and or data?
  • USERS

• What are some recommended security policies every organization should adhere by in order to prevent future attacks and outbreaks?
  • Real Education
  • Exercises
  • Even then it will fail.
Contact

Bret Padres
Director, Digital Forensics

(202) 464-5800

bpadres@strozllc.com

Stroz Friedberg – www.strozllc.com

New York, NY - Los Angeles, CA - Boston, MA - Washington, DC - Minneapolis, MN - Dallas, TX