PENETRATION CASES SHOW NEED FOR RESPONSE PLANS

by M. E. Kabay, PhD, CISSP-ISSMP

In my last column, I offered information security personnel cases of inadvertent data exposure to use in memoranda of justification for computer incident response plans. Here are some examples of deliberate penetrations that made the news in 2005.

* * *

In January, George Mason University reported that crackers stole personal information about 30,000 students, faculty and staff. <http://tinyurl.com/4nqb9>

A credit-card company alerted the DSW Shoe Warehouse to unusual activity; investigation revealed a data theft over three months that netted the thieves 1.4 million (1.4M) credit card numbers and information about shopping habits for customers of over 100 stores. <http://tinyurl.com/dgkek>

In March and April, LexisNexis announced exposure of the personal data of first 32,000 and then 310,000 US citizens in a series of 59 breaches in 2003 through 2005. <http://tinyurl.com/borg5> [Note to Trekkies: RESISTANCE IS FUTILE]

Polo Ralph Lauren’s customer database was hacked in April and the credit card information for at least 180,000 people was stolen. <http://tinyurl.com/cpu3d>

Tufts University sent letters to 106,000 alumni alerting them to the possibility of a data security breach involving their data. <http://tinyurl.com/aedew>

In May, a massive data theft was uncovered when police arrested nine people, including a collection agent who paid bank workers at Wachovia Corp., Bank of America, and two other banks for financial records on about
700,000 customers. <http://tinyurl.com/cft3o>

In July, evidence surfaced that a credit-card broker called CardSystems Solutions of Tucson, AZ was keeping archival data about transactions in violation of its agreements with clients. Data about 40M accounts were involved, of which 200,000 credit-card accounts may have been compromised. In June, plaintiffs launched a class-action lawsuit against Card Systems, VISA and MasterCard for failing to protect the data and for delaying notification of the victims. <http://tinyurl.com/bo3wd>

In August, the United States Air Force personnel system was penetrated using a stolen userID and password. More than 33,000 service personnel’s records were compromised. <http://tinyurl.com/8lgdg>

Also in August, criminal hackers broke into University of Colorado systems for the third time in six weeks. They compromised personal data including SSNs about 29,000 students, some alumni and 7,000 staff. <http://tinyurl.com/785t2>

University of Georgia revealed in September that criminal hackers compromised the SSNs of 1,600 people through unauthorized access to a university database. <http://tinyurl.com/8pard>

In December, Guidance Software of Pasadena, CA, makers of the well-known EnCase digital forensic software, suffered a penetration by criminal hackers who compromised the financial and personal data of 3,800 customers, including law enforcement personnel and security professionals. <http://tinyurl.com/b7c8n>

* * *

If your data were compromised by criminal hackers, how would you respond? Are your plans in place -- and tested -- for

* locking down the affected systems at once,
* notifying the appropriate law enforcement agencies (with whom you have already established good working relations),
* capturing digital evidence safely to provide iron-clad usability for forensic
analysis and in court,
* establishing a secure chain of custody for digital evidence,
* identifying the vulnerabilities exploited by the attackers,
* repairing the security holes to prevent new penetrations,
* coordinating corporate response to ensure a professional, accurate and timely flow of information to stakeholders?

Copyright (c) 2006 M. E. Kabay. All rights reserved.