Data Breach an All-Too-Often Occurrence

As Clive started his typical Wednesday morning routine, he was checking his e-mail. He saw a familiar name in his inbox. It was Jane, an information technology (IT) security manager at a competitive company. Clive and Jane have a good working professional (and ethical) relationship in which they often share information relating to security breaches and issues. Clive opens the e-mail, eager to see what new attack Jane has found. But in this case, Jane is pointing Clive to a pastebin link that contains the customer database content from Clive's company.

Clive is now in a panicked but controlled state. His mind starts to race. How did these data get from the company database to this Web site? Who did it? What systems were compromised to generate this list of data? Clive takes a moment and composes himself, and then he begins to analyze the situation.

The first task Clive does after he settles down is to inform the appropriate people. He calls his manager and tells her of the situation, and assures her that he and his team are analyzing the situation and will keep her informed of progress. Clive's next calls are to the team leaders of the network, database, and system administration organizations. The incident response plan is initiated.

Initial assessments from the three team leaders report the following:

- **Network:** After review of the intrusion detection system and firewall logs, there appears to be no abnormal activity; no alerts were generated.
- **Database:** After a review of database accounts, user and data definition (DDL) and data manipulation (DML) audit logs and database integrity checks, the database appears to show no abnormal activity.
- **System administration:** The system integrity checks and system audit logs show no abnormal activity.

After reviewing the reports, Clive is skeptical of the results, and he asks the teams to verify and confirm that log cleanup and deletion did not take place, and all leaders confirm that to be the case. Clive reports these findings to the management team. They are not pleased. They ask, "If no sign of break-in can be detected, then how did the list get generated and leave company premises?"

The incident response team heads back for more investigations. They next decide to review the application that the company uses. The application is an off-the-shelf application with a full and rich feature list. The various organizations use the features and insist that all of them are needed. Upon

review and investigation, they find that there are several pieces to the application that are not actively used by any team, yet certain people in the company have access to them. When reviewing these applications, a little hidden feature is found that allows users to write and run raw structured query language (SQL) statements in the database using the database application accounts.

The incident response team is curious about this feature and starts to investigate this path as the possible source of the data breach. Unfortunately, the application does not have auditing enabled for this area in the application. But the database administrator declares that there might be something that he can investigate.

The database auditing is only for DDL and DML, so SELECT statement access is not monitored, but the database does store all executed SQL statements in the Data Dictionary. A review of this information shows 1 query:

```
SELECT *
FROM app.customers;
```

All other statements accessing the app.customer table utilize a WHERE clause to limit the data to specific customers. The incident response team reviews this information and agrees this is how the data were extracted. Clive takes this information and reports back to the management team. They are pleased to know that progress is being made, but demand to know who did it and what can be done to prevent it from happening again in the future. The team now faces a new set of questions that need to be addressed:

- How was this access given?
- Who performed the SQL?
- How did it leave the company and make it to the pastebin site?

The incident response team added a new member to assist. The application support team was brought in and briefed on the situation and was asked to find out who performed the SQL statement and how he or she did it. Unfortunately, the company has all employees log in to a shared application account. The application does not offer detailed connection logging. It was determined that there are 2 departments with about 25 people who have the access to perform the task in question.

The human resources (HR) organization was engaged and conducted interviews with all 25 employees, but in the end, no one was found to have

conducted the data breach, and the incident was closed with no employee blamed for the incident.

In the meantime, while accountability was being reviewed, the incident response team had the obligation to resolve the incident. Two major resolutions were implemented:

- The application in question was modified, and direct SQL access was revoked.
- Generic accounts were no longer permitted; all users were now given named user accounts.

Moral of the Story

The use of software products without a full review of the application features and functionality led to the breach described in the story. In addition, the implemented access control model created accountability. A full review of any implemented software package needs to take place, and an understanding of all features and functionality is critical. Those features that pose a security risk should be disabled.

The use of the generic account with no additional auditing provided no accountability to the users for their actions. In this case, no one was ultimately held to blame for the incident except for the infrastructure and application support team for the lack of controls. The use of granular access controls is fundamental to any implementation.

In the end, the addition of a data loss prevention (DLP) network appliance could have alerted the company about the event. DLP devices monitor the network and look for data in motion and if sensitive data is detected alerts are raised. In this event, the large amounts of customer data being transmitted from the database to a client computer—and then potentially from the client computer out to the Internet—might have been detected.

Finally, security personnel must remember that not all security breaches are conducted from the Internet by expert hackers. The majority of incidents result from employees of the company performing malicious or, in most cases, accidental activities.