Detecting, Analyzing and Responding to Security Incidents: A Qualitative Analysis

Rodrigo Werlinger, David Botta, Konstantin Beznosov

University of British Columbia, Vancouver, Canada
{rodrigow, botta, beznosov @ece.ubc.ca}

1. INTRODUCTION

Persistence and cost are the two factors that have motivated several studies about better practices for dealing with security incidents [5]. However, there is not much literature about IT professionals who have to deal with security incidents, in terms of which tasks they actually perform and which resources they need to handle the complex scenarios given by real incidents [6]. This lack of research makes it difficult to evaluate and improve the support that IT security professionals need to respond efficiently to security incidents.

This study investigates how security practitioners deal with security incidents. To do so, this study adopted an exploratory posture, using ethnographic techniques [7] — questionnaires and interviews — to capture security practitioners' perspectives during security incidents.

Our poster will present the project, the design of the field study of security incidents, and the results of the study with the analysis of 13 interviews to security practitioners. These results include (1) the tasks performed by security practitioners during security incidents; (2) the skills and tools necessary to deal with security incidents; and (3) strategies that we consider to be required resources for dealing with security incidents.

Our preliminary results suggest some recommendations for the development of security tools: more focus on correlation of multiple sources of information, including the activities of different projects in distributed environments; and better trade-off between portability and visualization.

2. METHODOLOGY

The approach used in this study is based on ethnographic techniques. The use of ethnography made it possible to study security practitioners in the context of security incidents within their organizations. The ethnographic data were analyzed using grounded theory [3].

The ethical approval for contacting participants, the recruiting process, the interviews themselves and their transcriptions, were managed in the context of the HOT Admin project [2]. This project's field work provided 24 questionnaires and 14 interviews of IT security professionals with responsibilities in IT security. All the interviewees came from British Columbia, and most of them (12) were from academic organizations.

The analysis started with selecting data that pertains to security incidents [1]. About 13 situations related to security incidents were identified. The tasks performed and the resources used during the security incidents are described in the next section.

3. RESULTS

3.1 Security incidents mentioned by participants

The open-ended interview questions did not explicitly ask about security incidents. However, every participant talked about security incidents.

The most common incidents reported were related to malicious software. Within this type of incident, our participants distinguished between specific types of malicious software (trojan, malware, worm), the quantity of compromised machines, the type of asset compromised (user's PC or internal Host), and the regularity of the event.

Incidents related to Human Resources were mentioned in terms of the violation of internal policies. These incidents were characterized by the sensitivity of the internal communications during their investigations.

Phishing was a type of incident mentioned by one of the two participants in the private sector.

Suspected security incidents include those incidents that either were being investigated and there was no clarity about their causes, or those incidents that could materialize serious compromises in the future. These incidents were interesting because the participants needed to perform more tasks and use more resources and skills to discover the source of the problem.

3.2 Tasks

Table 1 shows the main tasks performed by our participants during the security incidents. These tasks were grouped in three main stages: detection, analysis and response. These stages account for the temporal sequence, since a security

[1]A security incident was considered as: "any real or suspected adverse event in relation to the security of computer systems or computer networks " [1]. The aspects of security considered were confidentiality, integrity and availability [4]

SOUPS July 18-20, 2007, Pittsburgh, PA, USA

Table 1: List of tasks performed during a security incident

Stage	Task
Detection	Monitor systems or networks Receive notifications
Analysis	Verification Assess the incident Track the source of the attack Collect more data to find the source of the problem Interact with other specialists Generate action plan Evaluate legal implications
Response	Turn off ports or services Clean-up systems Re-initialize services Patch or reconfigure systems System's restoration Administrative sanctions

incident is "perceived" by the security practitioner until a concrete action to stop it is taken. In between, during the analysis, security practitioners have to perform several tasks to confirm the incident, assess its scope, and find out the source of the problem or the attack.

3.3 Resources

3.3.1 Tools

A recurrent example of tools was the use of Shell/Perl scripts written by the same security practitioners to look for specific patterns of suspicious activity in firewalls and IDSs' log files.

There were also specialized tools to monitor networks and virus activity (IDSs, Antivirus). To analyze the packets of the network and find out the source of the attack or the problem, tools like TCPDump and Ethereral were used.

3.3.2 Skills

Pattern recognition: Pattern recognition was a recurrent skill that our participants had to use specially during the detection stage.

Hypothesis generation: Two participants had to generate hypothesis about those incidents where the cause of the problem was not clear.

Cooperation: Our participants had to cooperate and communicate with others for different reasons: make a more efficient investigation, execute specific actions in-situ, gather network information, interact with other specialists who had experienced similar problems or incidents, design a response plan to clean-up systems infected by a virus, etc.

3.3.3 Strategies

Isolation: Isolation was a strategy used to either verify incidents or to find out what was causing the anomaly or the attack.

Simulation: To investigate security incidents, participants sometimes needed to simulate the compromise, either in a controlled environment or in the production network.

4. DISCUSSION

Our empirical establishment of the temporal stages of a security incident—detection, analysis, and response—provides a basis for investigating the kinds of knowledge and skill exercised in the respective stages.

There was no incident in which the same person performed all the tasks from detection to response. This underscores the need for a better understanding of the different roles involved, and how they interact.

Our preliminary analysis showed that there are several opportunities to improve those IT security tools used by our participants to perform their tasks. For example: (1) tools that correlate other sources of information, such as a project's inventories, with the results of monitoring networks and systems, would help to discard false positives in highly distributed environments; (2) use different types of files as inputs an outputs to make tools more flexible and usable in situations where time and bandwidth are constraints to transmit and charge large files; and (3) utilize visualization features to indicate flows and meaning of network traffic. A tool that employs and integrate these features could be used to analyze log files from different sources and provide more meaningful data to security practitioners.

5. CONCLUSIONS AND FUTURE WORK

Our categories of responses to security incidents are well-grounded in empirical evidence, and provide a reasonable basis for future research. Our results include a list of types of security incidents, a model for the tasks, the skills employed, and the strategies used during security incidents. We gained some insight into the stages of response to a security incident, the high-level interactions between different people during an incident, and issues around which to improve security tools.

Future research is expected to bolster and refine our understanding of the deployment of tasks with respect to different kinds of security incident. We expect to fill out our map of how the skills, strategies and distribution of responsibilities come into play over the sequence of tasks.

6. REFERENCES

[1] Computer Security Incident Response Team CSIRT web page (accessed Feb 2007), available at: http://www.cert.org/csirts

[2] HOT Admin project web page (accessed Feb 2007), available at: http://www.hotadmin.org

[3] Kathy Charmaz, "Constructing Grounded Theory", SAGE publications, 2006.

[4] Wikipedia, CIA triad web page definition (accesed April 2007), available at: http://en.wikipedia.org/wiki/CIA_triad

[5] Forum for Incident Response and Security Teams web page (accesed February 2007), available at: http://www.first.org/

[6] Eser Kandogan and Eben M. Haber, "Security Administration Tools and Practices", Security Administration tools and practices, O'Reilly, August 2005, chapter 18, ISBN: 0-596-00827-9.

[7] Fetterman, David M., "Ethnography, Step by Step", Applied Social Research Methods Series, Volume 17, second edition, 1998.