https://doi.org/10.48009/2_iis_2005_217-223

KNOWLEDGE NEEDS AND DATA SECURITY AS THEY APPLY TO NETWORK INTRUSION DETECTION SYSTEMS

Charles A. Mance D.Sc., Robert Morris University, Chuck.Mance@respironics.com
Jeanne M. Baugh Ed.D., Robert Morris University,baugh@rmu.edu
Daniel Rota Ph.D., Robert Morris University, rota@rmu.edu

ABSTRACT

This research examines users of network intrusion detection systems (NIDS) in an effort to identify their understanding of NIDS. Thirty participants were studied using a qualitative case study methodology. This study focused on security analysts and managers responsible for operations, implementation, and the management of network intrusion detection systems and patterns of knowledge awareness related to the technology. Knowledge levels were categorized using Bloom's Taxonomy of Cognitive Learning. This research provides recommendations for improving the level of knowledge in an effort to enhance the overall understanding of the technology, which in turn may strengthen data network security.

Keywords: Data Security, Network Intrusion Detection

INTRODUCTION

The focus of this research is the knowledge base of the analysts utilizing and managing Network Intrusion Detection Systems (NIDS). NIDS is a relatively new technology developed to combat the ever-increasing malicious activity associated with Internet traffic. The first commercial NIDS, Net Ranger, was released by the Wheel Group in 1994 [4]. Data as of January 1, 2004, indicates a 30% increase in Internet users from 2000 to 2001, a 24% from 2001 to 2002, and a 22% increase from 2002 to 2003. There also has been a 142% increase in reported malicious Internet incidents from 2000 to 2001, a 56% increase in malicious Internet incidents from 2001 to 2002, and a 68% increase in malicious Internet incidents from 2002 to 2003. With this increase in Internet users and the increase in reported incidents comes the need for better detection of malicious data traffic. Technologies other than intrusion detection systems that inspect data traffic do exist. However, these technologies typically address specific threats; for example, content filtering which can be applied to applications such as electronic mail or Internet traffic. These technologies inspect data packets entering or exiting a data network looking for specific patterns of known vulnerabilities.

The relative newness of network intrusion detection systems (NIDS) technology and the increasing number of malicious Internet incidents are indicative of the need for skilled, knowledgeable security analysts to identify and defend against undesirable cyber activities. The Internet community depends on a non-hostile environment to effectively communicate and conduct business. When suspicious data is detected by the NIDS, an alarm is generated to alert the system owners of the event.

One of the issues surrounding NIDS is the amount of data being monitored and the ability of the system to detect anomalies [1]. This phenomenon can be compared to the air we breathe and the impurities within it. In this analogy, our immune system is the NIDS. The air we breathe is the data, and the number of impurities contained in the air is the malicious data traffic. We go about

our daily lives inhaling impurities, and at some point we may become ill from any one of these. Our immune system, or inner NIDS, detects an intrusion and raises an alarm through an elevated temperature or a number of other indicators. A physician performs tests and, based on the results plus other information like similar illnesses and past medical history, makes a diagnosis and recommends corrective action. This is a relatively straightforward process of treating the illness based on a diagnosis of the symptoms. The NIDS functions in a similar fashion monitoring data and identifying potential malicious traffic. The data traversing the network is analogous to the air we breathe.

Structure of the Study

The initial phase of this study was a series of detailed one-on-one interviews with 30 members of the corporate workforce responsible for data networking; security professionals, security consultants; and managers responsible for these services. The one-on-one interview technique is appropriate when a holistic, thorough investigation is necessary [3]. The convenient sample candidates were individuals the researchers have worked with or have been associated with through memberships in various security and information technology organizations such as the Pittsburgh chapter of InfraGard and the SANS (SysAdmin, Audit, Network, Security) Institute. The random selection process was conducted by applying a random selection computer program written in Perl developed by a participant. The program was administered against the membership list provided by The Pittsburgh Technology Council. Through the process, fifty potential organizations were selected. Every participating organization uses network intrusion detection systems as a component of their security practice.

Study Analysis

During the analysis of this study, four levels of technical expertise and exposure to the technology of network intrusion detection systems (NIDS) surfaced. In relation to the theoretical proposition, the researchers identified these as the engineer or technician (T), the manager (M), the executive (E), and the consultant (C). Progressing through this study, different silos of awareness based not only on various analysts and management levels within the sample set, but also between occupational specialties within the sample set began to arise. These fifteen themes were fundamental to the skill levels and the complexity of technology. These fifteen themes are as follows:

1. Technology awareness - is every participant was aware of network intrusion detection systems at some level?
2. Conceptualization - interpreting information in an abstract manner.
3. Application of the technology - separation from the technology and the level of understanding
4. Breaking down the data - what is done with the data produced and how often this data is reviewed and acted upon.
5. Synthesizing the output of the technology - combining output data in an effort to formulate or identify potential malicious data traffic.
6. Assessing the security landscape - knowledge level necessary for assessment, as well as understanding the corporate vision.
7. Managing expectations - what can the technology do
8. Valuing the Technology and the Protected Assets - how does one justify the technology

9. Data collaboration - Collaboration can take place between sources such as firewall logs, NIDS logs, and systems syslogs.
10. Configuration and tuning the technology - Using the pattern matching technique, the way a network intrusion detection system (NIDS) identifies potential malicious traffic
11. Monitoring and maintenance - multiple perspectives are addressed
12. Staying current with signatures – understanding digital patterns
13. Validity of the technology- will it do what it claims to do?
14. Future of the Technology – will the technology become obsolete?
15. Technology providing a false sense of security

Taxonomy of Knowledge and Awareness

This additional stage of the data analysis was included to enhance validity by introducing an external concept to further substantiate the findings. The intent was to categorize the case study findings in a format that would qualify the knowledge levels. For this, the researchers selected Bloom's Taxonomy as the basis for categorization. The six levels of Bloom's Taxonomy are: Knowledge; Comprehension; Application; Analysis; Synthesis; and Evaluation. Table 1 provides the relationships between these six levels of Bloom's Taxonomy, and the participants' knowledge levels as they applied to NIDS.

Table 1. Relationship between Bloom's Taxonomy and Knowledge Levels Relating to Network Intrusion Detection Systems

Bloom Level	Example	Relationship to Research
Knowledge	*Understand technical vocabulary* - e.g., firewall, signatures, vulnerabilities, TCP/IP - ability to articulate functionality of the technology *Develop knowledge of major ideas* - definition of technology and related concepts - identification of limitations of technology	Technology Awareness
Comprehension	*Understand information* - a high level understanding of vulnerabilities *Grasp meaning* - understanding the implications of vulnerabilities and the effect on the environment as related to the technology *Translate knowledge into new context* - demonstration of awareness of existing security posture - demonstration of awareness of the impact on the security posture in reference to the technology *Interpret facts, compare, and contrast* - evaluation of NIDS capabilities between various vendors and platforms *Predict consequences* - evaluation of security posture by component and in its entirety	Conceptualization
Application	*Use information* - use of existing security infrastructure to implement technology *Use methods, concepts, theories in new situation* - implementation of the technology applying gained knowledge of systems and operations *Solve problems using required skills or knowledge* - proper application of the technology	Applying the Technology
Analysis	*See patterns* - recognition of valid and suspect data patterns *Organize parts* - consolidation of segmented data for further analysis *Recognize hidden meanings* - identification of hidden meanings within data streams	Breaking Down the Data

	Identify components - identification of components of data packet and interpretation of the information contained within	
Synthesis	*Use old ideas to create new ones* - Utilization of existing patterns and signatures to develop new in an effort to anticipate future vulnerabilities *Generalize from given facts* - ability to deduce from minimal data *Relate knowledge from several areas* - triangulation of data from multiple sources to identify traffic patterns *Predict, draw conclusions* - identification of new malicious traffic patterns from systems data	Synthesizing the Output of the Technology
Evaluation	*Compare and discriminate between ideas* - determination of validity of data against predefined signatures, therefore further eliminating false positive responses *Assess value of theories, presentations* - verification of proper alarming of signatures *Make choices based on reasoned argument* - use of knowledge from prior experiences *Verify value of evidence* - ability to confirm source of malicious data when possible *Recognize subjectivity* - ability to play the devil's advocate by challenging assumptions; turning tacit theory into concrete concepts	Assessing the Security Landscape

As technology becomes more complex, there is a potential need for more specialized skill sets. In order to properly apply network intrusion detection systems (NIDS) technology in the current environment, there is a need for specialized skill sets at the analyst level.In addition, there is a need for a higher level of knowledge awareness at the management level, which encompasses a broader yet less detailed knowledge level.

The first level, Knowledge, signified closeness to the technology and a knowledge need. The next level, Comprehension, was another level of knowledge needed. Level three, Application, represented a further separation from the technology and an additional level of needed knowledge to actually apply network intrusion detection systems. The remaining three levels implied a further separation from the technology and additional levels of needed knowledge. The theoretical proposition focused on specific skills applicable to separation from the technology.

Bloom's Taxonomy of Cognitive Learning provided the device to identify the different levels and a mechanism by which to qualify. Table 2 represents the overall findings at a high level. An X in a cell represents participants having the necessary skills associated with a particular relationship. As the table indicates, the knowledge needs of technologists span all six levels of the Bloom model.

Table 2. Knowledge Needs as applied to Bloom

	Engineer/Technician	**Consultant**	**Manager**	**Executive**
Knowledge	X	X	X	X
Comprehension	X	X	X	X
Application	X	X	X	X
Analysis	X	X	X	X
Synthesis	X	X	X	X
Evaluation	X	X	X	

The participants responsible for the day-to-day operations of the technology had the most comprehensive knowledge and understanding of network intrusion detection systems. From their perspective as it relates to Bloom's Taxonomy, the following skills are associated with the technologist needs: intimate knowledge of the technology and limitations; thorough understanding of vulnerabilities and how to identify them; ability to implement, monitor, and maintain network intrusion detection systems in accordance with security industry best practices; ability to properly analyze and synthesize multiple data sources in an effort to identify potential malicious data traffic; ability to evaluate findings and determine validity.

The knowledge needs of managers are similar to that of the engineers and technicians with exception of the shared responsibilities subsets. Managers in the shared responsibilities subset area need only possess knowledge of the technology and its limitations, and an understanding of the vulnerabilities and their potential impact to an organizat When looking at patterns of knowledge, two distinct patterns emerged. Pattern One was applicable to the full time security analysts and associated levels of management. In order to sell a service, a high level of knowledge is required throughout the organization. Pattern Two was applicable to organizations that employed the technology, but without data security as their main focus. In these cases, the requirements were not as demanding with respect to NIDS.

CONCLUSIONS, RECOMMENDATIONS, AND IMPLICATIONS

The relative newness of network intrusion detection systems (NIDS) technology and the increasing number of malicious Internet incidents are indicative of the need for skilled, knowledgeable security analysts to identify and defend against undesirable cyber activities. The fact that different levels of awareness exist within this technology implies a deficit in data security knowledge awareness. Several reasons can be attributed to these conclusions—budgetary constraints, staffing limitations, unawareness of Internet vulnerabilities, lack of training, staff turnover, and time to train. An explanation of these reasons could be the rapid rate of technological change. One area that affects data security is the value of the data. In all data security initiatives, there is a trade off between spending to secure data versus what data is being secured. These numbers vary depending on whom within the organization is questioned. As identified in this study, the emergent theme of Valuing the Technology and the Protected Assets produced different responses from the engineers/technicians, the managers, the executives, and the consultants.

To better understand the technology and how it is deployed, the following eight recommendations are presented:

1. Define the Technology.

The first step in developing recommendations is to define the technology, such as Personal Digital Assistants (PDAs), cellular phones, or Instant Messaging (IM). Defining the technology ensures a consistent starting point in identifying what the technology is designed to do.

2. Identify the Limitations of the Technology.

The next step is to identify the limitations associated with the technology. It is not enough to know what the technology can do. What the technology cannot do is just as important and is often overlooked. These first two steps require a high level of knowledge about the technology.

3. Determine the Need.

Once the technology has been defined and the limitations have been identified, the next step is to determine if there is a need within the organization. For technologists, it is important to evaluate from a point of view other than a technology perspective. For instance, a company's international sales force requires mobile communications. Does that company provide cellular phones equipped with global positioning system (GPS) technology and digital cameras imbedded, or does it provide prepaid calling cards? Every situation may not require a complex technological solution.

4. Determine the Fit.

Fit is addressed here not only as a physical fit within the security landscape, but also as staffing and cultural consideration. As a physical fit, an organization must ask, "Where does the technology sit within the network?" In order to determine the physical fit, a thorough knowledge of the current infrastructure is required. This includes egress and engress points of data; services and applications offered, such as Internet portals; and all protocols and applications running over the networks. From a staffing perspective, an organization must ask, "Do we have the right human capital to properly implement, monitor, and maintain the technology?" Management must decide whether the technology is going to support an around-the-clock environment. In order to be effective, network intrusion detection systems must run 24 hours a day, 7 days a week. Therefore, when determining a fit to the staff, this needs to be considered. This fit consideration should be the determining point as to whether to host the technology in house or to outsource.

5. Determine the Training Needs.

Whether hosted internally or externally, the technology needs to be fully understood. Internally, employee skills are necessary in order to properly deploy the technology. Externally, analysts and managers need to understand the technology to ensure the external provider is providing what was contracted. The training needs identified at a minimum should include data networking, networking protocols, operating systems, network infrastructure, security policies, security components, vulnerabilities, and intrusion detection systems.

The security analysts for the categories of dedicated security specialists and shared responsibilities should possess all six Bloomian levels of competencies for all eight training categories in order to properly utilize network intrusion detection systems (NIDS). Managers should also possess all six Bloomian levels of competencies for all eight training categories for the categories of dedicated security specialists and shared responsibilities in order to properly utilize NIDS. The executives responsible for supporting network intrusion detection systems as a shared responsibility should possess knowledge and comprehension, the first two levels of Bloom competencies for all eight training categories. The recommend competencies for the executive organizations are data security-centric. Although this group is focused on providing data security solutions to other organizations, the need for the executives to synthesize and evaluate does not exist. Consultants should possess all six Bloomian levels of competencies for all eight training categories in order to properly design, implement, and support data security initiatives. Consultants are expected to have a high level of expertise; therefore, these competencies are essential.

6. Provide Ongoing Maintenance and Support.
An added component of every technology is the ongoing maintenance and support. Failure to properly maintain and update systems will impact the functionality of security systems, which can allow malicious traffic to penetrate the network perimeter and provide a false sense of security.

7. Perform Security Audits.
Security auditing provides validation and verification of the technology and of the security policies. Auditing should be provided by an outside source, and the results should be reviewed with all parties.

8. Stay Active in Communities of Practice.
The researchers believe that one of the best ways to stay current with security issues is through communities of practice. Staying active in the security community provides a forum to express concerns and exchange ideas.

The Security Paradigm, or Network Security vs. Secure Networks
Is network security provided by a secure network, or is a secure network provided by network security? Network security here is defined as an organization's staff responsible for implementing security initiatives. A secure network is the result of the efforts of a network security team. Without proper knowledge and training, neither network security nor secure networks can exist.

The security paradigm is in a state of flux, and will continue to be so. Industrial requirements and knowledge needs vary from technology to technology and application to application. Brown and Duguid state this paradox eloquently. "People attempting to buy knowledge in one form or another often face a curious dilemma. If they can evaluate it, they probably don't need it. If they need it, they probably can't evaluate it" [2, p. 215]. Stated otherwise, the perception of what industry requires is relative to who has the requirement.

While the technological future is a great unknown, the technological present is bound only by human imagination—which in itself is boundless—implemented for good or evil. It is paramount for organizations to be prepared for the technological future by arming themselves today with appropriately knowledgeable experts at every level of knowledge need.

REFERENCES

1. Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J. and Stoner, E. (2000). *State of the practice of intrusion detection technologies.* http://www.sei.cmu.edu.pub/documents/99.report/pdf/99tr028.pdf
2. Brown, J. S. & Duguid, P. (2000). *The social life of information*. Boston, MA: Harvard Business School Press.
3. Feagin, J, R., Anthony M. O., & Gideon, S. (1991). *A Case for the Case Study.* Chapel Hill: University of North Carolina Press.
4. Innella, P. (2001). *The evolution of intrusion detection systems*. http://www.securityfocus.com/infocus/1514