Security Policies in Military Environments

Mojca Ciglaric, Andrej Krevl, Matjaz Pancur and Tone Vidmar
University of Ljubljana, Faculty of Computer and Information Science
Trzaska 25, SI-1000 Ljubljana, Slovenia

{ mojca.ciglaric, andrej.krevl, matjaz.pancur, tone.vidmar } @fri.uni-lj.si

Saso Tomazic, Ales Zavec
University of Ljubljana, Faculty of Electrical Engineering
Trzaska 25, SI-1000 Ljubljana, Slovenia

{ saso.tomazic, ales.zavec } @fe.uni-lj.si

Stanko Ciglaric
Slovenian Institute of Quality and Metrology
Trpinceva ul. 39, SI-1000 Ljubljana, Slovenia

stane.ciglaric@siq.si

ABSTRACT

Security has always been a topic of attention in military environments. However, with the advances in technology, the ever-growing number of various electronic devices that surround us, and the complexity of these devices, the security risks are also greatly increasing. Traditionally, military environments have a tight physical security, but sometimes lack a good security policy for the numerous electronic devices that are used not only in the field, but also in the office. As these devices are becoming easier to use, we cannot neglect the potential human abuser who does not need great expertise in the field of electronics or computing to gain access to confidential data, either from the outside or from the inside of the system. The paper proposes a system for managing and formally specifying security policies for electronic equipment as well as for other areas that require a security policy. Further, it discusses problems with integrating local legislation and local policies with policies of alliance partners (e.g. NATO) or policies based on bi-lateral and multi-lateral agreements, with the objective of the union policy not only conforming to all the other policies, but also enhancing and superseding them. On the other hand, the paper focuses on the potential attacks from within the system and discusses the teaching techniques that can help to establish a level of knowledge that provides the required level of security in accordance with the sensitivity of the data used during any process. The paper shifts the focus from various security devices to the ever increasing importance of the human factor in systems with sensitive data.

1.0 INTRODUCTION

Security is becoming increasingly important in information systems of today. Cyber criminals are better organized than ever and their attacks are carefully planned and even paid for. They do not rely only on software bugs like they used to. They use advanced attacking techniques and social engineering to gain as much information as possible before compromising the systems. Thus it is impossible to protect information systems only by means of security hardware. The pressure is being put on information technology specialists to educate their users and create security policies that would enable protection of

Ciglaric, M.; Krevl, A.; Pancur, M.; Vidmar, T.; Tomazic, S.; Zavec, A.; Ciglaric, S. (2006) Security Policies in Military Environments. In *Dynamic Communications Management* (pp. 19-1 – 19-8). Meeting Proceedings RTO-MP-IST-062, Paper 19. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

the data throughout the business process. As we will present in our quick overview of the most common attacks on modern information systems, the weakest link in today's information systems are people, not buggy software. We show the complexity of a corporate security policy through the introduction of security polices and continue to propose a security policy management system that enables security policy managers to organize and regain control over their security policies. The security policy management system features a security knowledge cycle that forces employees to continually educate in the area of security thus improving overall security of our information systems.

2.0 INFORMATION SECURITY

Information security is characterized as the preservation of confidentiality (information accessible only by authorized people), integrity (data remains accurate and complete) and availability (authorized users can access information when needed) [6, 7]. When a security threat uses a resource's vulnerability, any of the three information security aspects can be compromised. Vulnerability is a weak point of a resource that enables us to use that resource for malicious activities. Vulnerabilities vary from software bugs, to weak passwords or an unlocked toolbox. It is important to point out that vulnerability by itself does not represent a security risk to the system. Threats can be divided into random threats like earthquakes, floods, fires and deliberate threats like data theft, secret agents, malicious software and similar. When a threat uses a vulnerability of a resource, it poses a security risk to the system.

As the purpose of this paper is not to give a comprehensive list of all attacks on information systems, we will just quickly revise the most common ones.

2.1 Attacks from the Internet

The most common attacks on computers that are connected to the Interned exploit software bugs in application that listen for traffic from the internet. Software bugs usually cause buffer overflows that enable execution of arbitrary code. We can protect ourselves from this type of attacks by setting up firewalls between our computers and the Internet. Firewalls filter incoming and outgoing traffic and prevent malicious traffic from reaching our computers. Although firewalls are efficient, they are not enough as attackers will try to compromise the services required for our daily operations as we still let those bypass the firewall. We can prevent such attacks only by patching our software with bug fixes regularly.

When the traffic leaves the corporate networks it can be subjected to sniffing (unauthorized traffic inspection) by a third party. That is why we need to encrypt the data we send over the public Internet. Keep in mind that sending an unencrypted e-mail through the Internet is like sending a postcard via regular post – everyone can see what has been written on the postcard.

2.2 Social engineering

Our information systems can be compromised even if we patch our systems regularly. Modern attackers use social engineering to gain access to restricted systems. They combine legitimate services like e-mail and web sites with naivety of uneducated computer users. Social engineering attacks vary from mass e-mailing of malicious attachments with inviting names like "iloveyou.doc" to password theft and to carefully planned company infiltrations in form of fake employees, fake telephone calls, fake salesmen and fake websites all used to gain access to the organization's computer systems.

2.3 The “inside job”

Since security hype hit the media and the industry we have all learned to run our firewalls, to run the latest version of the antiviral software and to patch our systems regularly. Companies pay big money for corporate firewalls and proxies that carefully inspect the traffic going to and coming from the Internet. We have tight password restrictions and group policies, yet all our computers have USB ports with no access restrictions. Nowadays it is actually cheaper to bribe an employee in the company to bring us wanted information on a USB key that trying to hack the same company’s information system from the Internet. Since most system administrators trust the users of their networks to behave ethically and morally it is easy to sniff data of the corporate networks and access other user’s files. Social engineering is even easier inside a company. How many times have you copied a file from your computer for your co-worker just because “his boss said so”.

Some of these attacks cannot be prevented by even the most expensive security hardware whilst they can be easily dealt with if we develop a sensible security policy and educate our users about security and information technology.

3.0 SECURITY POLICIES

Security policies are a special type of business rules that indicate a course of events or a way to handle a situation [1]. Policies declare what “must” and “must not” be done in an organization and can be thought of as a law specific to the organization. Security policies should be precise, consistent and comprehensible as they apply to each and every worker in the organization. Each task that takes a course of actions not compliant with the security policy should obtain special approval prior to its executions and if such approval is not granted the task leads to a security incident. The scope of a security policy is not limited to an organization as it extends to business partners cooperating with our organization – even the tightest security in our organization will not protect our data if our business partner leaks that information in the wild.

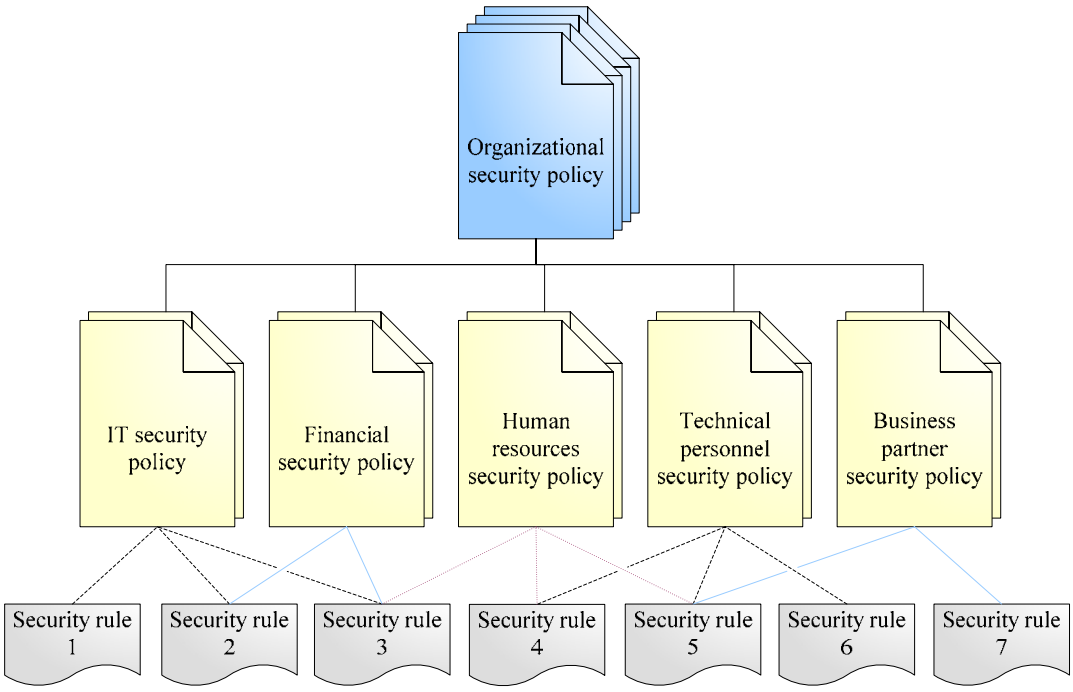

Figure 1: Security policy hierarchy.

There is some confusion to what security policy actually is since we are referring to both a single business rule and a corporate document with multiple business rules with the same term. We will refer to a security policy that defines a single rule or a single course of actions as a security rule and we will call the document that comprises of all the security rules in a company a corporate or organizational security policy. Since organizational security policies can span several hundred pages [1] it is useful to define security policy documents that apply only to a certain role or a certain department and contain only the subset of all the security rules in the organizational security policy. Figure 1 shows relations between security rules, security policy documents and organizational security policy. While security policy documents do not reference each other, a single security rule can be contained in many different security policy documents. However an organizational security policy can contain either all of the security policy documents or all of the security rules.

Since security policies are a number of rules written in several documents they are (much like our legislation) hard to manage and to enforce. Some of the policies can be implemented with controls like door locks, fire alarms, firewalls etc. Other policies may require a new type of a business role like a security officer that checks all employees for photo-id badges when they enter the premises of the organization. Yet most of the security rules rely on people and their acquaintance with the security policy. So with all the wonderful security devices (firewalls, biometric devices, security cards etc.) available on the market today the security of our organizations falls back on the human factor and its ability and willingness to understand and comply with the security policy.

3.1 Formalization

Any kind of automation is practically impossible if security policies are kept in our natural language. That is the reason why researches have developed different languages for security policy formalization. They all rely on a model that represents a view of the system at a given point [8]. Today, most notable security policy formalization languages are Ponder and XACML.

In Ponder, a security policy is a rule that can be used to change the behaviour of the system [9]. Ponder supports authorisation policies, delegation policies and obligation policies. Authorisation policies specify what a subject is permitted or forbidden to do on a set of target objects. Obligation policies specify what a subject must do to a set of target objects. Delegation policies specify which actions a subject can delegate to other subjects. Objects and subjects can be grouped in a domain and security policies can be then applied to the whole domain at once. Listing 1 shows a Ponder specification of a security policy disallowing all secretaries except Jane to print on “OurColorLaserJet” between 3 p.m. and 8 p.m.

```
inst auth- SecretaryPrint {
     subject /staff/Secretaries - /staff/Secretaries/Jane
     target /resources/printers/color/OurColorLaserJet;
     action print() ;
     when Time.between("1500", "2000");
}
```

Listing 1: Security policy in Ponder

With the growing popularity of extensible markup language (XML) another standard for security policy formalization the extensible access control markup language (XACML) emerged. Similarly to Ponder, XACML provides basic constructs like <Resource>, <Actions>, <Target>, <Subjects> which can be combined into a <Rule> specifying that subject may or must interact with certain targets or resources. Like most XML documents XACML is harder to read by humans (the rule specified in Listing 1 spans beyond a whole page). However, the XACML specification is developed by OASIS which makes it very likely to be included in future software that will enable security policy automation.

But even an extensible language cannot embrace every security rule in an organization. And even if it could, do we want our security guards to master Ponder in order to check workers' photo-id badges when they come to work every morning?

4.0 SECURITY POLICY MANAGEMENT SYSTEM

Security policies are a complex issue. Organizational security policy is divided into several department security policy documents which may further define security policy documents for different roles in the department. These documents include a number of security rules that may also be included in other security policy documents. Formalization and automation are not suitable in most cases so we have to rely on our workers to comply with the security policy and also to help enforce it. However people will (by nature) feel that all of the security mechanisms required by the security policy are used just to get in the way of their work and to render them less productive. That is why our workers need to be well educated why security policy is needed and why it is in their best interest to comply with it. This means that not only do our workers need to read the security policy they also need to understand it.

Since we have already mentioned that full automation of security policies is not possible we are proposing a security policy management system (SPMS) that will at least lessen the complexity of dealing with security policies in an organization with implying certain workflows and enabling automation where possible.

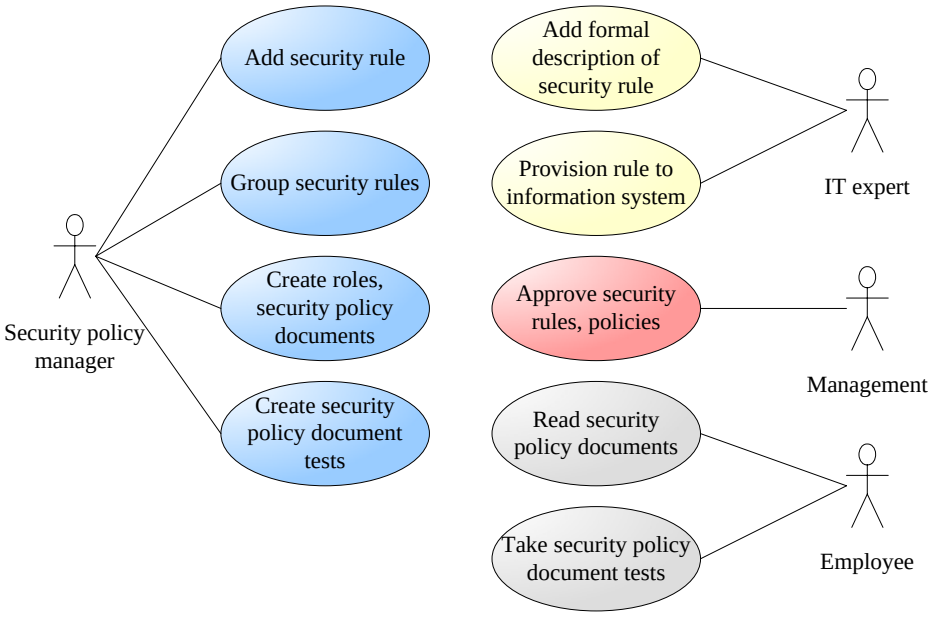

Figure 2: Usage of SPMS

4.1 SPMS use cases

Figure 2 shows typical use cases of the SPMS. A chief information officer, a pre-specified body or a similar role uses the system to add new security rules to the rule database. These are entered in text (natural language) and may have images, video or voice attached for better understanding. A security rule can also include hyperlinks to similar rules and to standards or technical documents that define how a rule should be implemented. The same actor can also create roles (that can be equal to job positions) and security policy documents. These documents or roles enclose a set of security rules previously grouped together in the rule database. Finally several tests with questions on the security policy can be created for each policy document. These tests can be used to check whether our employees really understand the security policy and why it needs to be enforced.

Since all security policies need to be approved by the management the proposed system includes a use case that enables executives to approve each new security rule or each new security policy document before it is visible by employees in the SPMS.

Employees can access the SPMS at any time to read security policy documents related to their position in the organization. Additionally, the employees must also take periodic tests that check their knowledge on security policies. The tests cover only areas of the security policies related to their position in the organization.

If automation is possible an information technology expert can formalize a security rule and provision that rule to the software that allows security policy specifications. It has to be noted that provisioning modules should be developed specifically for the software in question.

4.2 SPMS Architecture

The SPMS is a web application. This greatly simplifies content delivery to clients (employees) as most of modern computer operating systems include a web browser. The web is also an ideal platform for distributing materials that educate employees about the impact of a security policy on the system. With the help of on-line tests the web application can also easily check the employee's knowledge on a certain policy and it can prevent cheating by randomizing questions and answer order.

All the data required by the web application is stored in a rule database. An ordinary relational database is used for this purpose as it provides all the functionality needed by the web application and it also enables us to use existing databases already set up in our system with no extra costs.

Formalized security policies can be provisioned to directory and access control servers that understand security policies. On the other hand an employee who has not taken the appropriate security policy tests related to his position in the organization could be automatically denied access to the organization's information system. Architecture of the SPMS is shown in Figure 3.

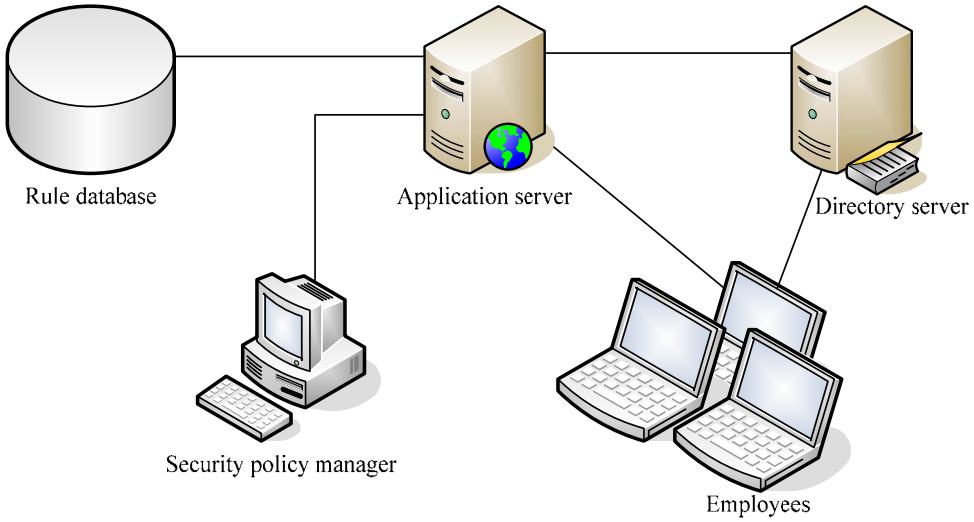

Figure 3: SPMS architecture

4.3 Security knowledge cycle

As we have already mentioned, nowadays the security focus needs to shift from security hardware to personnel education, training and general security consciousness. That is why we propose constant user education in the form of a security knowledge cycle. The security knowledge cycle starts early in the process of hiring a new employee at the organization. We need to educate the applicants on our security policies. If an applicant agrees to the security policy required for the position he applied to, he later takes the test to check if he understands the security policy properly. If he passes the test he is hired, otherwise he is further educated on the subject or dismissed from the job interview.

Once the applicant is hired he is subjected to testing his knowledge on security policies in pre-defined periods of time. If the employee passes the test, he may continue with his daily operations, if he does not pass the test he is further educated on the subject and he needs to take the test again. If an employee repeatedly fails to pass the test he is denied access to organization's information systems and dismissed from the organization.

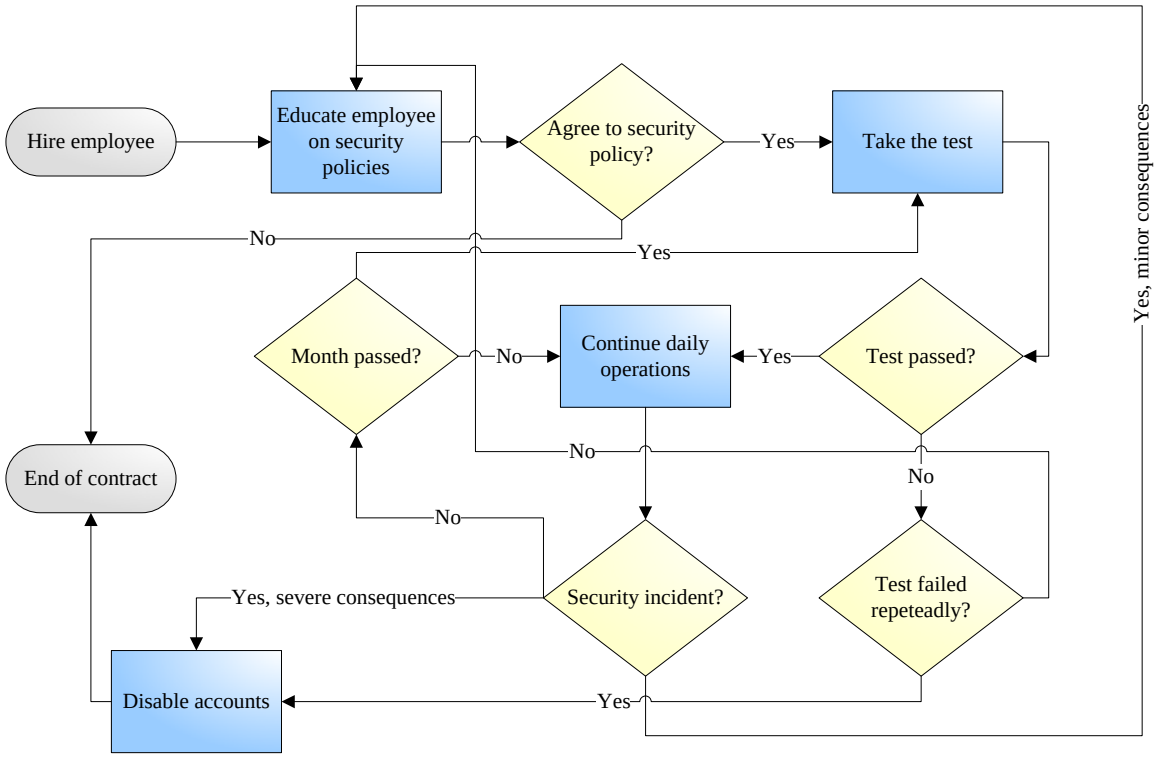

Figure 4: Security knowledge cycle

If an employee causes a security incident and the consequences of the incident are minor he is subjected to more training on security policies and he needs to take the tests again. However if the security incident has sever consequences on the organization's business processes, the employee is denied access to organization's information system and dismissed from the organization. Figure 4 shows the security knowledge cycle in detail.

5.0 DISCUSSION

We have shown that computer security is an increasingly important subject in today's information systems. As attackers are getting smarter and more organized, it is impossible to provide enough security only by buying security hardware and software. Our employees need to be educated on security subjects and they need to comply with the company security policy.

However building a good corporate security policy is a daunting task and without some sort of a management tool security officers will get lost in endless lists of security rules. That is why we have proposed a security policy management system that organizes our security rules and enables us to combine them into security policy documents and into corporate security policy. Besides security policy management, our proposal also includes a security knowledge cycle. This knowledge cycle ensures that our users actually know what the security policy they must comply with means and what are the consequences if they do not comply with it. Furthermore we can educate our employees on latest threats to prevent incidents in advance.

Security equipment by itself offers only limited security, but when combined with a good security policy and every employee's compliance with the security policy, the result can prove to be excellent.

6.0 REFERENCES

[1] C.C. Wood, Information security policies made easy, PentaSafe Security Technologies, Inc., 2002.

[2] T.R. Peltier, Information Security Policies, Procedures, and Standards, Auerbach Publications, 2002.

[3] S. Northcutt, L. Zeltser, S. Winters, K.K. Frederick, R.W. Ritchey, Inside Network Perimeter Security, New Riders Publishing, 2003.

[4] J. Scambray, S. McClure, G. Kurtz, Hacking Exposed, 2nd ed, Osborne / McGraw Hill, 2001.

[5] J. Mallery, J. Zann, P. Kelly, W. Noonan, E. Seagren, P. Love, R. Kraft, M. O'Neill, Hardening Network Security, Osborne / McGraw Hill, 2005.

[6] S. Tomazic, T. Vidmar, G. Kandus, M. Ciglaric, M. Pancur, A. Krevl, A. Zavec, A. Kos, Pregled napadov na informacijsko komunikacijski sistem : projekt "Viking", University of Ljubljana, 2005.

[7] S. Tomazic, T. Vidmar, M. Ciglaric, M. Pancur, A. Krevl, A. Zavec, A. Kos, Varnostne politike in standardi varovanja informacij : projekt "Viking", University of Ljubljana, 2005.

[8] S. Tomazic, T. Vidmar, M. Ciglaric, M. Pancur, A. Krevl, A. Zavec, A. Kos, Formalizacija varnostnih politik: project "Viking", University of Ljubljana, 2005.

[9] N. Damianou, N. Dulay, E. Lupu, M. Sloman, Ponder: A Language for Specifyinf Security and management Policies for Distributed Systems, Imperial College, Department of Computing, 2000.