УДК 004.7.056.53

I.V. Kotsiuba, post-graduate
Pukhov Institute for Modeling in Energy Engineering of NAS of Ukraine
(15, General Naumov St., Kyiv, 03164, Ukraine
e-mail: i.kotsiuba@gmail.com)

Human-insider Threat Analysis for the Purpose of Modeling

This article presents the definition of the insider threat and its impact; it also provides an overview of techniques to control and remediate these threats.

Дано определение инсайдерской угрозы и рассмотрены ее воздействия. Представлен обзор методов контроля и способов устранения этих угроз.

K e y w o r d s: insider threat, integrity, BYOD, vulnerability.

Introduction. A major driver for insider threats stems from the motive and intent of an employee to perform a malicious activity for either financial gain or personal satisfaction.

An insider threat is no longer associated with privileged account management or operational superusers. Engineering, development and system administrators are often associated with having the ability to perform data processing activities and execute transactions that few others are permitted to perform. Threats are also associated with general users, due to a lack of clearly defined controls and policies that help delineate separation of duties, data-in-transit activities and access-deprovision processes.

The risk associated with data loss, for example, does not always coincide with malicious activity. The rise of Bring Your Own Device (BYOD), or simply the introduction of corporate-managed smartphones, has also opened up another attack vector, in which sensitive emails and corporate information can be lost either via negligence or device theft or interference.

While each enterprise has its own infrastructure, personnel and business processes, this is a staggering percentage attributable to employees who are responsible for development, protection and executing of business processes that should aid in the enterprise growth.

Insider threat increases as an enterprise's infrastructure and complexity of interaction increase. In today's ever-connected work and social landscape, the risk of information dissemination is as high as ever.

The rise of home-based working and BYOD has not only increased flexibility and, arguably, efficiency, it has also opened up an avenue of information flow that, if not well managed and maintained, can be a great liability. The main area of concern is the general employee who has a basic level of IT understanding, and also has a limited grasp of IT and information security. This lack of understanding is likely to cover the vast majority of employees and can put information at risk in the simplest way, e.g., a home worker who allows family members to use a work laptop or the company mobile to download an untrusted app.

The rise of BYOD also opens up the opportunity for users at the opposite end of the technical spectrum to become an information liability.

The true impact of insider threats is largely unknown. This is mainly due to an enterprise's inability to identify, track, report and remedy the data breaches that occur within the corporate landscape.

From the perspective of information system, an external intruder who gains access actually becomes the insider. To avoid false reasoning, we introduce the concept of "Insider process". So, the insider process – is executing user's process on whose behalf illegitimate actions are produced. This definition covers activities within information environment as an insider and external intruder. It is worth to note that these illegitimate actions can be established only by content, while remaining legitimate by form.

Until recently, the main focus in the construction of information security was to prevent external threats [1]. Most of the companies were limited to software installation, protect information systems from external influences such as remote gaining unauthorized access to information, the installation of malicious software, etc. Such security has evolved constantly increasing level of resistance to such attacks, losing, meanwhile, the possibility of impact on the system from the inside. Until recently, the problem of internal threats was not attached due importance. While struggling with the external intruder protection system in an attempt to gain access to information, the insider receives this information quite freely within its competence or illegally expanding their rights and opportunities.

The concept of "insider" covers a fairly wide range of offenders, but their general feature is that all these people have legal access to information systems and perform illegal actions in it. It is important to note that the term "insider" does not necessarily imply malice offender. As an example, the ordinary employee, who for his own convenience or entertainment installs on your computer, connected to the company network, programs not provided by the company security policy, or visits the untrusted Internet resources. The installed programs may not have the appropriate level of security, and visited sites contain malicious code that in the end, can be exploited from outside. Thus, the employee may disclose confidential information "without knowing it".

For critical infrastructures, that kind of attacker is a dramatically growing threat [2]. There are attackers with different motives and expertise and could cause different levels of damage to the network. Attackers could be script kiddies, elite hackers, terrorists, employees, competitors or customers.

The attackers can be divided into 5 groups:

1) Non-malicious attackers who view the security and operation of the system as a puzzle to be cracked. Those attackers are normally driven by intellectual challenge and curiosity.

2) Consumers driven by vengeance and vindictiveness towards other consumers making them figure out ways to shut down their home's power.

3) Terrorists who view the smart grid as an attractive target as it affects millions of people making the terrorists' cause more visible.

4) Employees disgruntled on the utility/customers cause unintentional errors.

5) Competitors attacking each other for the sake of financial gain.

There are cases when insiders become out of ignorance or out of good intentions. An example of the latter is a company secretary, who received a call from a superior officer to transmit sensitive information via email to the specified address. The man who introduced himself as the chief may be an intruder, and said email — address of a competing company. Thus, the Secretary becomes an insider on the basis of the best reasons, without knowing it.

In these examples, the insiders are just a tool to get information for real intruders. Such cases are not uncommon, but the main danger is posed by insiders, which aim is to produce malicious action to take the benefit of financial or moral satisfaction.

Actions of insiders, to succeed, almost always, ultimately entail financial losses for the organization. In order to be able to detect an insider must first understand what it may represent a threat. There are seven basic types of insider threats [3, 4], representing a violation of the principles of information security — confidentiality, integrity and availability.

Confidentiality:

Leakage of confidential information.

Bypass means of protection against leakage of confidential information.

Theft of confidential information by negligence.

Infringement of copyright in the information.

Integrity:

Fraud, the substitution of some other resource.

Misuse of company's information resources.

Availability:

Sabotage of IT infrastructure — either intentionally or spontaneously.

In the context of insiders the threat of leakage of confidential information means the following: owing to the actions of insiders important information is

transferred to people who have no access to this information. This threat can be conducted in many different ways, for example, via email, USB-memory or a printer. To prevent such threats the company should apply filtering internet-traffic control at the workstation level, archiving corporate correspondence and administrative constraints (blocking P2P channels at the level of the firewall).

The threat of bypass leakage protection of confidential information implies the possibility to cheat the system security. For example, an insider who knows about the existence of email message filters, can try to change the sent information so that his letter would not arouse suspicion. However, this type of threat is only possible with a legacy system and weak protection methods because it is impossible to avoid modern security system virtually in this way.

Negligence, carelessness or ignorance of the employees may pose a threat to steal confidential information inadvertently. In this case, an insider with public information may inadvertently put sensitive data on a web page that is accessible to the public, or copy sensitive information on a portable storage medium that is: it will subsequently be lost or stolen.

It is also worth to notice that an insider with no malicious intent, faced with the inability to make conceived action will not try to circumvent the protection system, which greatly facilitates the suppression of this class of threats.

The threat of copyright violation on the information, in general, involves the use of information by insider without the owner's knowledge. Use of information from one author's letters without attribution; use of materials published on the Internet without treatment, in their instruments; installation of illegal software distribution; fake sender's email address in order to create a false impression of him — all these are examples that can produce the threat of copyright infringement on the information. Control operations are performed on workstations to prevent this type of threat. In general, the problem of preventing illegal copying is very acute and there is no comprehensive solution. Several areas of protection, such as "electronic watermark" only emphasize the problem complexity.

The threat of fraud in the informational environment involves the possibility of misuse of important changes to the company's data. In this case, an insider can act like a user who has no access to this information and receives it illegally, and staff members with a right to get information do not even notify superiors. For example, an accountant, spontaneously changing wage of employees, is an insider, realizing the threat of fraud. To eliminate this type of threat the companies use widely the control of financial reporting, monitoring user activity, etc.

The threat of misuse of the information resources of the company is very extensive and versatile. The implementation of this type of threat involves actions committed by a network that is not under its workflow. Examples of such actions are: sending advertising messages, visiting entertainment web pages, the use of

improper language in business correspondence. The mechanisms of mail messages and web traffic filtering are applied to prevent such threats.

The threat of sabotage in IT infrastructure is mainly used by persons whose motivation is personal. It may be, for example, resentful employees who choose to hurt the company in which they work by any way possible. The essence of a threat is that an insider with access to the system, trying to destroy it, destroys important information with injecting viruses, etc. Successful implementation of this threat has often very serious consequences for the company and entails serious losses, and takes time to restore the system. Protection against such acts should cover two aspects: first, the monitoring of the working atmosphere and corporate conflicts, and secondly, technical limitations of the actions of each employee.

At the moment, there is no single set of security tools that will prevent all of the threats used by insiders, but there are remedies that eliminate one or more of these threats. Therefore, the actions of insiders are the least preventable with using the developed information security tools. In the next section we consider the ordering of insiders' actions to identify the most characteristic features of the system undergoing invasion. These features will be used by us in the choice of model parameters of monitoring the computer system.

Analysis of insider's activity. In order to identify insider's ways to harm the information system, you must cover (if possible) all possible insiders' scenarios. Classification and models of insiders and their actions can significantly reduce the number of scenarios of actions to be taken into account. In the context of this work the division of insiders into certain types supposedly allows us to correlate their actions with the change of some specific parameters of information systems under the supervision of ISS. Such research can help to justify theoretically the relationship between the attacker and incident detected in the computer system.

There are many models and classifications of insiders. The most common are the following.

One of the first classifications of insiders was proposed in 2006, by the international research company IDC [3]. The division of intruders in this classification is made on the basis of their loyalty to the company. On this basis, all insiders are divided into four classes: "citizens", "intruders", "departed" and "traitors".

The first class, "citizens", consists of the most loyal employees, which almost do not violate the security policy set in the information environment. These employees become intruders accidentally or because of inexperience. People belonging to this class can bring minimal or even no threat to the system.

The second class, "intruders", is the most numerous. It includes all employees whose actions deviate from the accepted security policy, but are entertaining

or personal. Examples of such actions are visiting during working hours the outside Internet resources, playing computer games, chatting online, and others. Insiders belonging to this class represent a threat to the information system, but in most cases losses related to incidents that occurred through the fault of these individuals are insignificant.

The third class, "departed", includes people who spend most part of their time, committing acts that constitute gross violations of security policy. For example, these steps include: installation and use of unauthorized software, publication of confidential information on a variety of online resources, as well as other misuse of the connection to the Internet. Attackers belonging to this class of intruders are a serious threat, and their actions can greatly affect the well-being of the company in which they work.

The fourth most disloyal class of insiders, "traitors", is the most dangerous, since it includes persons intentionally subjecting the information system to the threat of confidential information. "Traitors" are often motivated by material benefit, so their actions are well thought out, careful, invisible and carry serious harm to the company. Examples of such actions may be deliberate entering the malware in the local network, database and theft of intellectual property. Effects of "traitors" can be extremely serious, up to the bankruptcy of the injured party.

The above classification covers all insiders; however, it is too inexact, and the boundaries between its classes are blurred and conventional. This classification does not apply to solve the problem raised in this paper. The actions of insiders of this classification are difficult to correlate with changes in certain parameters of the system, since the same actions can be performed by representatives of different classes. In addition, this classification criterion is the motivation of insiders that does not reflect the potentialities of representatives of individual classes in respect of the system and is of more general educational character.

The other classification of insiders was offered by research company InfoWatch [3]. It differs from the classification according to IDC by clearer boundaries between classes, by their more complete description, as well as by taking into account not only the attacker's motivation, but also the nature of his impact on the system. According to this classification, any insider can be attributed to one of the following six classes: "careless", "manipulated", "offended", "disloyal", "earning" and "embedded".

The class of "careless" insiders includes people who violate the established rules in the information environment by accident or on the basis of their own "best" reasons. This class includes the majority of ordinary workers. For example, an employee becomes a "careless" insider, when copying confidential information to external media in order to finish the job at home, and loses a carrier, thus providing access of strangers to this information. Faced with the impossibi-

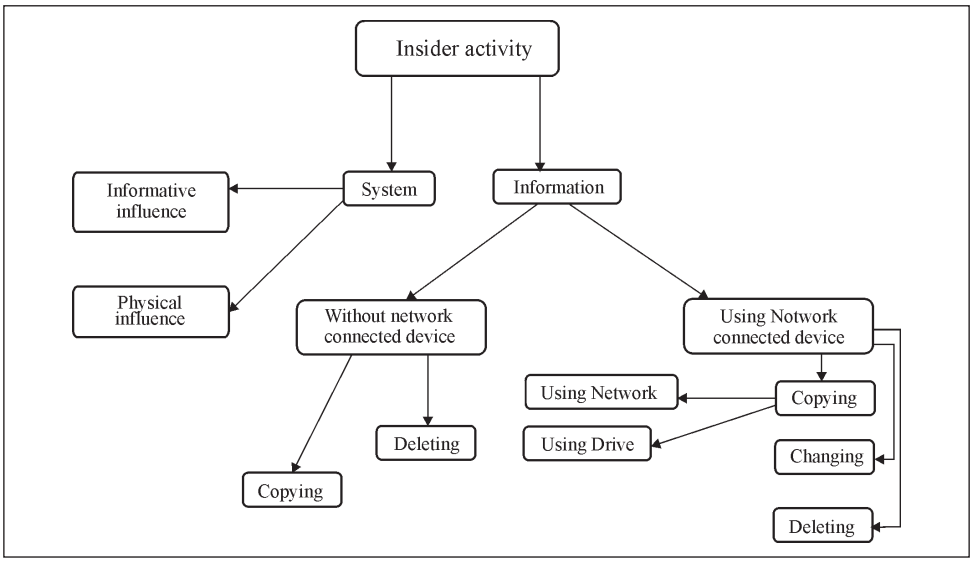
lity to commit an illegitimate act, such offender is likely to ask his colleagues for help. Thus, employees belonging to this class of insiders create undirected threats and their malicious actions are unmotivated. Despite the considerable number of acts generated by this class of insiders, the great number of threats remains unfulfilled and does not involve any losses.

The class of "manipulated" insiders consists of loyal people who commit illegal actions in respect of the information system under the influence of outsiders. In most cases, this class includes employees who are victims of various types of fraud, including social engineering. For example, if an employee, who has received an email from a superior officer with a request to send confidential information to an external email address, follows these instructions, he/she becomes a "manipulated" insider, as an attacker could forge the sender's address, thereby misled the said employee. Threats from "manipulated" insiders can cause considerable harm. The considered two classes of internal intruders in common include people which are not intended to break rules, unlike the subsequent classes.

The class of «offended» insiders includes people who commit illegitimate actions for personal reasons. The actions "offended" insiders are destructive, that is, they tend to harm the information environment and not to steal information. For example, if an employee, who was refused of increasing wages, decides to take revenge of the company where he works by storing malware in the company network or by theft of company's confidential information for its competitors, he falls into the class of "offended" insiders. The considered type of malice creates a very dangerous threat to the information system, because when faced with failure, they will try again to do harm until they are disclosed or until they reach the desired result.

The feature of insiders, members of the class of "disloyal", lies in the fact that their illegal actions are motivated, in the first place, by the desire to gain benefit in exchange for information (in general) to which they have access when working in the company. Unlike attackers included in the previous class these offenders have no personal motives and are not intended to harm the current employer, they are driven by calculation. The examples of such insiders are people who are going to change their place of work and in order to take advantage at the subsequent work take certain confidential information such as customer's database. The actions of these insiders realize the threat of information theft and, depending on the importance of information stolen, the consequences can be extremely unprofitable.

The class of "earning additionally" insiders covers offenders who initially were loyal to the organization in which they work, but for some reason, began to make malicious acts on behalf of disloyalty to persons of the mentioned organi-



Insider activity

zation. In most cases, the reason for such action is the desire for material benefit for the actions taken. The most common example of such offenders is a member of the organization who has access to confidential information, whom a competitive company offered a cash prize for this information, and who accepted their conditions. Threats brought by such offenders are most dangerous, because the insider has a reputation of a very loyal person, and it is difficult to track his illegitimate actions, though they are directional.

The class of "embedded" insiders is similar to the previous one, with the difference that in this case the attacker initially aims to make malicious actions related to processes of organization. Threats brought by this class are similar malicious threats mentioned in the description of "earning additionally" insiders.

The above classification of internal attackers is much more informative than the classification according to IDC. However, despite the fact that in a certain sense the classification types of actions are recorded as those made by insiders. Firstly, in the previous classification the same action can be accomplished by hackers belonging to different classes, but in this case the number of classes is mainly downward. Secondly, the observed types of actions do not reflect exactly what manipulations are made in the computer system, which are critical in determining the variable parameters of the system. Due to the fact that the use of existing classifications of insiders is impractical, the need arose to offer new systematization of insiders' actions.

Earlier it was noted that in the context of information system, an external intruder who gains access to the above system actually becomes an insider. To avoid false reasoning, we introduce the concept of "insider process". So, the insider process — an executable system of user process on which behalf the insider produced illegitimate actions. This definition covers the process in which insider or intruder wants to be granted with access to the information system. It is worth to notice that these illegitimate actions, as mentioned earlier, can be defined while they are still legitimate. Thus, further in this paper, all actions of insider towards IS we call insider process.

In order of systematization the violator has been effectively applied to solve the problem identifying ISS in the information system by monitoring its condition, it must meet the following requirements:

arrangements are to be made to take into account all (if possible) types of the insider actions with respect to the information system;

systematization should have clear boundaries between various actions of the offender and projected changes in the information system functioning.

Based on these requirements, the author proposed a model of insider misconduct shown in Figure. According to this scheme, any insider's action can be, first of all, directed to the information system, which is obviously reflected either in the parameters of the observed system or in information contained in the information systems.

REFERENCES

1. Zegzhda P.D. and Rudina E.A. (2008), *Osnovy informatsionnoy bezopasnosti* [Fundamentals of information security], Politechnicheskiy Institut, S. Petersburg, Russia.
2. Kravtsov, H., Kotsiuba, I. and Prytulyuk, I. (2015), "The cybersecurity modeling in critical infrastructures", *Elektronnoe modelirovanie,* no. 4, pp 75-84.
3. Skiba, V.Y. and Kurbatov, V.A. (2008), *Rukovodstvo po zaschite ot vnutrennikh ugroz informatsionnoi bezopasnosti* [Inside information threat prevention manual], Piter, S. Petersburg, Russia.
4. Stolfo, S.J., Bellovin, S.M. and Hershkop, S. (2008), Insider attack and cyber security beyond the hacker, California, Springer, USA.

Received 25.02.16

KOTSIUBA Ihor Vasylyovych, post-graduate student of the Pukhov Institute for Modeling in Energy Engineering of NAS of Ukraine; graduated from the State University of Information-Communication Technologies in 2010. Field of research: posterior methods for analysis of threats of information security.