ISSN 2411-1031. Information Technology and Security. July-December 2015. Vol. 3. Iss. 2 (5)

INFORMATION SECURITY

УДК 004.056.53

VOLODYMYR MOKHOR,
HRYHORII KRAVTSOV,
IHOR KOTSIUBA

ASSESSMENT OF INSIDER ATTACK WITH LEARNING STATISTICS METHODS

The popularity of mobile devices, wearable devices used in collaborative information systems, has dramatically exploded over the past decade. Thus, we understand that in ordinary office, a single person can use plenty of active interfaces like wireless data transfer interfaces, which can help, among direct usage, strengthen access control and information security subsystem. Despite the fact that enterprises quite rightly develop controls and prevention techniques to combat cyberattacks, threats from users within the corporate network pose a significant risk to information assets. Existing users with accounts, permissions and access required to perform their jobs are increasingly becoming a major risk to information security through account misuse, data loss and fraudulent activities. This article reviews the definition of an insider threat and its impact, and provides an overview of the techniques to control and remediate these threats.

Keywords: 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 a 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 different infrastructure, personnel and business processes, this is a staggering percentage attributable to employees who are responsible to develop, protect and execute business processes that should aid the growth of the enterprise.

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, external intruder who gains access actually becomes insider. To avoid false reasoning, we introduce the concept of «Insider process». So, insider process – is executing user’s process on behalf of whom there are being produced illegitimate actions. 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 was 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 did not attach due importance. While struggling with the external intruder protection system in an attempt to gain access to information, 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 who 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 their own convenience or entertainment installs on your computer connected to the company network, programs not provided by the company security policy, or visit the untrusted Internet resources. Installed programs may not have the appropriate level of security, and visited sites contain malicious code than in the end, can be exploited from outside. Thus, the employee may disclose confidential information without knowing it.

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

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. Are seven basic types of insider threats [2], [3], representing a violation of the principles of information security – confidentiality, integrity and availability.

Confidentiality:

1. Leakage of confidential information.
2. Bypass means of protection against leakage of confidential information.
3. Theft of confidential information by negligence.
4. Infringement of copyright in the information. •

Integrity:

1. Fraud, the substitution of some other resource.
2. Misuse of company's information resources

Availability:

1. Sabotage IT infrastructure - either intentionally or spontaneously.

In the context of insiders under the threat of leakage of confidential information means the following: from the actions of insiders important information transferred to the people who do not have 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 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 information being sent so that his letter was not to arouse suspicion. However, this type of threat is only possible with a legacy system and weak protection methods because modern security system virtually impossible to avoid 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 – 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 insiders information without the knowledge of its owner. Use for one author in his letters, without attribution; use without treatment, in their instruments of materials published on the Internet; installation of illegal software distribution; fake sender 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. To prevent this type of threat is used controls operations on workstations. In general, the problem of preventing illegal copying is very acute and is not a comprehensive solution. Several areas of protection, such as «electronic watermark» only emphasize the complexity of the problem.

The informational environment threat of fraud involves the possibility of misuse of important changes to the company's data. In this case, an insider in this case can act like a user who does not have access to this information, and get it illegally, and staff members with a right to do it, but without ever notifying superiors. For example, an accountant, spontaneously changing wage of employees, is an insider, realizing the threat of fraud. To eliminate this type of threat is widely used controls 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 action 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. To prevent such threats apply filtering mechanisms mail messages and web traffic.

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 to inject the virus, 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, the 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 using developed information security tools. In the next section we consider the ordering of actions of insiders to identify the most characteristic features of the system undergoing invasion. These features will be used by us in the choice of model parameters monitoring computer system.

Insider activity analysis. In order to identify ways to harm insider information system, you must cover (if possible) all possible scenarios insiders. 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 division insiders on certain types of supposedly allow to correlate their actions with the change of some specific parameters of an information system under the supervision of ISS. Such research can help to justify theoretically the relationship between the attacker and the incident is detected in the computer system.

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

One of the first classifications insiders was proposed in 2006, an international research company IDC [2]. Separation 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».

First class «citizens», consists of the most loyal employees, almost do not violate the security policy set in the information environment. Intruders these employees become accidentally or inexperience. People belonging to this class are minimal threat to the system or do not represent it at all.

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 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 of their time, committing acts that constitute gross violations of security policy. For example, these steps include - installation and use of unauthorized software, the 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, pose a serious threat, and their actions can greatly affect the well-being of the company in which they are located.

Fourth, the most disloyal class insiders – «traitors», is the most dangerous, since it includes a person intentionally subjecting the information system and the threat of confidential information. Often motivated «traitors» is a 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 of 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, is too inaccurate, and the boundaries are blurred between her classes and conventional. This classification does not apply to solve the problem raised in this paper. This is due to the fact that the actions of insiders classification is 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, the criterion for this classification is the motivation of insiders that does not reflect the possibility of representatives of individual classes to the system and is being more general educational character.

The second deals with the classification of insiders was offered by research company InfoWatch [2]. It differs from the classification according to IDC clearer boundaries between classes, a more complete description of them as well as take into account not only the motivation of the attacker, but the nature of its 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».

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 said carrier, or access to it strangers. Faced with the impossibility to commit an illegitimate act, such offender is likely to ask for help to colleagues. Thus, employees belonging to this class of insiders create undirected threats and malicious actions of their unmotivated. Despite the considerable amount generated by this class of threats posers, the vast number of these threats remain unfulfilled and do not involve any losses.

Class «manipulated» insiders consists of loyal people who commit illegal actions in relation to 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 to an external email address confidential information shall comply with these instructions, it becomes a «manipulated» the insider, as an attacker could forge the sender's address, thereby misled the said employee. Threats outgoing from «manipulated» insiders can cause considerable harm. Considered two classes of internal intruders in common is that the people involved in them, are not intended to break the rules, unlike the subsequent classes.

In the class of «offended» insiders includes people who commit illegitimate actions for personal reasons. Basically 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 refused to increase wages, decides to take revenge of the company where he works, by storing malware in company network or theft of confidential information and of its competitors, it falls into the class of «offended» insiders. Consider the type of malicious creates a very dangerous threat to the information system, because when faced with failure, they will try again harm until they are found or until their actions do not lead to the desired result of.

Feature insiders, members of the class of «disloyal», lies in the fact that their illegal actions motivated in the first place, the desire to benefit in exchange for information (in general) to which they can 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. Examples of these insiders can serve people who are going to change their place of work, and in order to take advantage of the subsequent device to work, since they take a certain confidential information such as customer 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.

Class «earning additionally» insiders covers offenders who initially were loyal to the organization in which they work, but for some reason, began to make a malicious act on behalf of disloyalty to the organization mentioned persons. 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, which competes company offered a cash prize for giving them this information, and that takes their conditions. Threats posed by such offenders are the most dangerous, as an insider in the past could establish itself as a very loyal person, and his illegitimate actions becomes difficult to track, but at the same time they are directional.

Class «embedded» insiders is similar to the previous class, with the difference that in this case the attacker initially aims to make malicious actions in relation to the implemented within organization. Threats posed by this class are similar malicious threats mentioned in the description of «earning additionally» insiders.

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

Earlier it was noted that the position information system, an external intruder who gains access actually becomes insider. To avoid false reasoning, we introduce the concept of «insider process». So, insider process – an executable system user process on behalf of which produced illegitimate actions. This definition covers activities in the information environment as an insider and external intruder to access this system. It is worth emphasizing that these illegitimate actions, as mentioned earlier, can be established only content, while remaining legitimate form. Thus, later in this paper, referring to the actions of insiders in the information environment, we mean the insider process, unless specified otherwise.

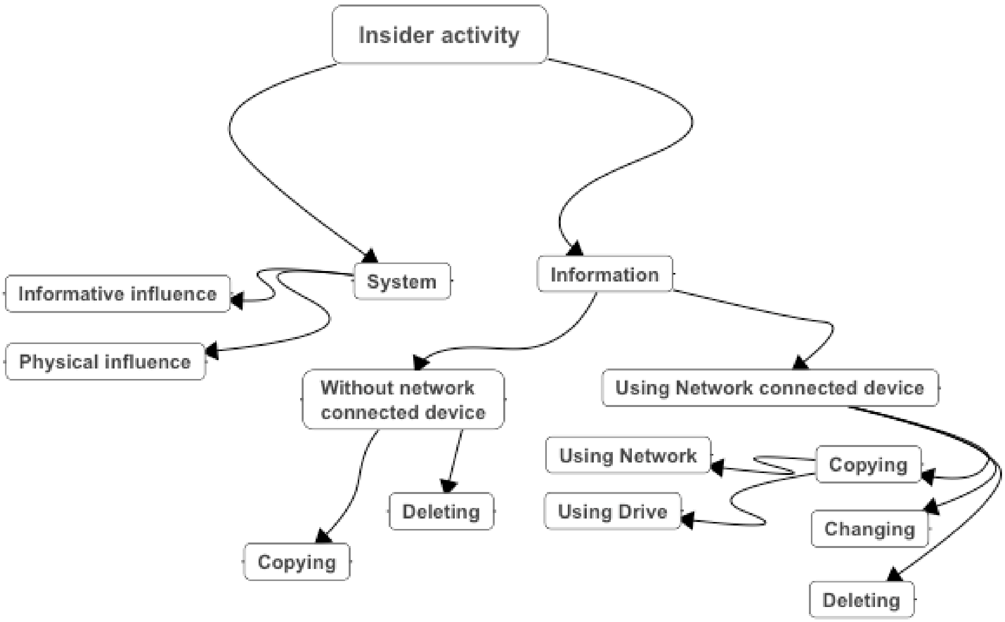

Figure 1 – Insider activity

In order to systematize 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 taken into account all (if possible) types of actions insider with respect to the information system;

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

Based on these requirements, the author proposed a model of insider misconduct shown in Fig. 1. According to this scheme, any action insider, first of all, can be directed either to the information system, which is obviously reflected in the parameters of the observed system or the information contained in the information systems.

REFERENCES

1. Zegzhda, P.D., Rudina, E.A. (2008), *Osnovy informatcionnoi bezopasnosti* [Basic Information Security], Polytechnic Institute Publ., Snt. Ptrsb., 224 p.

2. Skiba, V.Y., Kurbatov, V.A. (2008), *Rukovodstvo po zashchite ot vnutrennikh ugroz informatcionnoi bezopasnosti* [Inside threat prevention manual], Piter Publ., Snt. Ptrsb., 320 p.

3. Stolfo, S. J., Bellovin, S. M. (2008), *Shlomo Hershkop: Insider Attack and Cyber Security Beyond the Hacker,* Springer Publ., California, 223 p.

The article was received 05.10.2015.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Зегжда П. Д. Основы информационной безопасности : конспект лекций / П. Д. Зегжда, Е. А. Рудина. – СПб. : Изд-во Политехн. ун-та, 2008. – 224 с.

2. Скиба В. Ю. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба, В. А. Курбатов. – СПб. : Питер, 2008. – 320 с.

3. Stolfo S. J. Shlomo Hershkop : Insider Attack and Cyber Security Beyond the Hacker / S. J. Stolfo, S. M. Bellovin. – California : Springer, 2008. – 223 p.

ВОЛОДИМИР МОХОР,
ГРИГОРІЙ КРАВЦОВ,
ІГОР КОЦЮБА

ОЦІНЮВАННЯ ІНСАЙДЕРСЬКИХ АТАК СТАТИСТИЧНИМИ МЕТОДАМИ НАВЧАННЯ

Популярність мобільних і портативних пристроїв, що використовуються у спільних інформаційних системах, стрімко збільшилась протягом останнього десятиліття. Таким чином, у звичайному офісі людиною може використовуватися велика кількість активних інтерфейсів. Таких як бездротові інтерфейси передачі даних, що може сприяти, у випадку безпосереднього використання, покращенню контролю доступу та підсистем забезпечення безпеки інформації. Незважаючи на те, що підприємствами розробляються методи контролю та попередження реалізації кібератак, загрози від користувачів, що знаходяться усередині корпоративної мережі, найбільш небезпечні для інформаційних активів через неправильне використання акаунтів, втрату даних або шахрайські дії. У статті розглядається визначення інсайдерської загрози та її впливу, а також пропонується огляд методів контролю та запобігання цим загрозам.

Ключові слова: інсайдерська загроза, цілісність, BYOD, уразливість.

ВЛАДИМИР МОХОР,
ГРИГОРИЙ КРАВЦОВ,
ИГОРЬ КОЦЮБА,

ОЦЕНКА ИНСАЙДЕРСКИХ УГРОЗ СТАТИСТИЧЕСКИМИ МЕТОДАМИ ОБУЧЕНИЯ

Популярность мобильных и портативных устройств, которые используются в совместных информационных системах, стремительно увеличилась на протяжении последнего десятилетия. Таким образом, в обычном офисе человеком может использоваться большое количество активных интерфейсов. Таких как беспроводные интерфейсы передачи данных, что может способствовать, в случае непосредственного использования, улучшению контроля доступа и подсистем обеспечения безопасности информации. Несмотря на то, что предприятиями разрабатываются методы контроля и предотвращения реализации кибератак, угрозы от пользователей, которые находятся в середине корпоративной сети, наиболее опасные для информационных активов из-за неправильного использования акаунтов, потерю данных или мошеннические действия. В статье рассматривается определение инсайдерской угрозы и ее влияния, а также предлагается обзор методов контроля и предотвращения этим угрозам.

Ключевые слова: инсайдерская угроза, целостность, BYOD, уязвимость.

Volodymyr Mokhor, doctor of technical sciences, professor, head of academic department, State institution «Institute of special communications and information security National technical university of Ukraine « Kyiv polytechnic institute», Kyiv, Ukraine.
E-mail: v.mokhor@gmail.com.

Hryhorii Kravtsov, candidate of technical sciences, doctoral student, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.
E-mail: java_dev@i.ua.

Ihor Kotsiuba, postgraduate student, Pukhov Institute for modeling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, Ukraine.
E-mail: i.kotsiuba@gmail.com.

Володимир Володимирович Мохор, доктор технічних наук, професор, завідувач кафедри, Державний заклад «Інститут спеціального зв’язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», Київ, Україна.

Григорій Олексійович Кравцов, кандидат технічних наук, докторант, Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України, Київ, Україна.

Ігор Васильович Коцюба, аспірант, Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України, Київ, Україна.

Владимир Владимирович Мохор, доктор технических наук, профессор, заведующий кафедрой, Государственное учреждение «Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», Киев, Украина.

Григорий Алексеевич Кравцов, кандидат технических наук, докторант, Институт проблем моделирования в энергетике им. Г. Е. Пухова Национальной академии наук Украины, Киев, Украина.

Игорь Васильевич Коцюба, аспирант, Институт проблем моделирования в энергетике им. Г. Е. Пухова Национальной академии наук Украины, Киев, Украина.

УДК 004.91:65.012.45

ЮЛІЯ КОЖЕДУБ

СТВОРЕННЯ ДОКУМЕНТАЦІЇ ДЛЯ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Запропоновано нову систему створення документації для систем управління інформаційною безпекою, що відображає особливості, притаманні системам управління інформаційної безпеки організації. Відображено аспекти, пов’язані з персоналом та їх поводженням з документами, що стосуються інформаційної безпеки підприємств та/чи організацій.

Ключові слова: документація, міжнародні стандарти, системи управління, управління організацією, персонал.

Постановка проблеми. Зважаючи на широке поширення систем управління на різні сфери життя й діяльності людини, і відносячи себе до шанувальників вище зазначених систем, висвітлюється власний погляд на означене питання.

Розроблення документів для потреб систем управління, зокрема для систем управління інформаційною безпекою, є важливе, якщо не найголовніше, питання функціонування організації і отримання прибутків, сталого його розвитку й безперервності бізнес-процесів.

Слід завжди пам’ятати, що усі дії персоналу у певній організації мають бути задокументовані. Їх записано у численній низці документів, що регламентують роботу як окремої людини (посадової особи), так і усієї організації, не забуваючи про проміжні документи, що стосуються роботи відділу, сектору, департаменту тощо. В такому разі унеможливлюються аврали, збої в роботі, термінові усунення неполадок на висхідному етапі, затримки у виконанні плану реалізації або зриви у постачанні продукції чи наданні послуг. Зрозуміло, що за відповідного розумного планування й виконання дій персонал зможе постійно звертатись до цих документів, де детально й реально відображено певні процедурні