Въведение и ключови понятия, свързани с информационната сигурност

Валентина Войноховска, Светлозар Цанков

Abstract: Key Concepts and Introduction to Information Security: *The paper represents an introduction and key concepts to information security. The essence of the information security, important characteristics of information and the components of the information system are explained in the text. The present document has been produced with the financial assistance of the European Social Fund under Operational Programme "Human Resources Development". The contents of this document are the sole responsibility of "Angel Kanchev" University of Ruse and can under no circumstances be regarded as reflecting the position of the European Union or the Ministry of Education and Science of Republic of Bulgaria. Project № BG051PO001-3.3.06-0008 "Supporting Academic Development of Scientific Personnel in Engineering and Information Science and Technologies".*

Key words: *Information, Security.*

ВЪВЕДЕНИЕ

Целта на информационната сигурност е защита на ценните ресурси (информация, компютърен хардуер и софтуер) на дадена организация. Чрез подбор и прилагане на подходящи предпазни мерки, сигурността подпомага мисията на организацията чрез предпазване на нейните физически и финансови ресурси, репутация, правна позиция, служители и други материални и нематериални активи.

За повечето организации сигурността на информацията и системите, които я обработват, предават и съхраняват е от изключително важно значение. В много организации информацията е бизнес.

Създаването на програма за информационна сигурност, която се придържа към принципите на сигурността като бизнес фактор, е първата стъпка в усилията на дадена организация при изграждане на ефективна стратегия за сигурност. Организацията трябва непрекъснато да:

- изследва и оценява рисковете за информационната сигурност на бизнес операциите;
- определя какви политики, стандарти и контрол трябва да се изпълняват за намаляване на тези рискове;
- насърчава информираността и повишаване на знанията и уменията на персонала;
- оценява съгласуваността и ефекта от управлението.

СЪЩНОСТ НА ИНФОРМАЦИОННАТА СИГУРНОСТ

Компютърните системи и мрежи са едни от най-високо технологичните продукти на човечеството. Освен всички предимства, които предлагат, те имат и редица недостатъци. Проблемите със сигурността под формата на зловредни програми, загуба на правото на неприкосновеност на личния живот, изпращане на нежелана реклама или спам, засягат почти всеки компютърен потребител. Следват три дефиниции на понятието *сигурност* [1]:

Дефиниця_1

Сигурността е свойство на една система да противостои на външни или вътрешни дестабилизиращи фактори, които могат да доведат до нейното нежелателно състояние или поведение. Това важи и за сигурността на информационните системи.

Дефиниця_2

В българския език терминът *сигурност* означава две различни неща, които могат лесно да се обяснят чрез английските думи – *security* и *reliability*. Първата

означава защита от неправомерни действия на хора или група от хора, а втората – защита срещу различни природни заплахи и проблеми с хардуера.

Дефиниция_3

Мерките, предприети с цел предпазване от шпионаж или саботаж, престъпност, атака или изтичане на информация.

Една успешна организация трябва да има следните няколко слоя на сигурност за защита на своята дейност:

- **Физическа сигурност** – защита на физическите обекти или области от неоторизиран достъп и злоупотреби.
- **Сигурност на персонала** – защита на хора или група от хора, които имат оторизиран достъп до организацията и нейните операции.
- **Сигурност на операциите** – защита на определена операция или серия от дейности.
- **Сигурност на комуникациите** – защита на средата за комуникация, технология и съдържание.
- **Мрежова сигурност** – защита на мрежовите компоненти, връзки и съдържание.
- **Информационна сигурност** – защита на конфиденциалността, интегритета и достъпността на информацията при съхранение, обработване или пренасяне. Това се постига с прилагане на политики за сигурност, обучение и повишаване на знанията и чрез помощта на технологиите.

ВАЖНИ ХАРАКТЕРИСТИКИ ЗА ИНФОРМАЦИЯТА

Стойността на информацията се определя от характеристиките, които тя притежава. Някои, от изброените по-долу, характеристики увеличават или намаляват стойността на информацията повече от други. Например [3]:

Наличност

Наличността позволява на авторизирани потребители – хора или компютърни системи да имат достъп до информация без възпрепятстване. Например, в библиотеките се изисква идентификация на читателите. Съдържанието на библиотеката е защитено така, че то да е достъпно само за авторизирани посетители. Читателите удостоверяват своята идентичност преди да получат безплатен достъп до книгите.

Акуратност

Акуратност на информацията има тогава, когато в нея няма грешки и неточности, и има стойността, която крайните потребители очакват да има. Ако информацията е била преднамерено или непреднамерено променена, тя вече не е прецизна.

Автентичност/Достоверност

Автентичност на информацията е качеството или състоянието й да бъде оригинална, а не възпроизведена или измислена. Информацията е автентична когато е на същото ниво, на което е била създадена, съхранена или предадена.

Конфиденциалност

Информацията е конфиденциална когато е защитена от разкриване или излагане на неавторизирани потребители или системи. Конфиденциалността предполага, че само такива с права и привилегии за достъп биха могли да я използват. За защита на информацията могат да бъдат прилагани множество мерки, които включват:

- Класификация на информацията.
- Сигурно съхранение на документи.
- Прилагане на общи политики за сигурност.

- Обучение, както на служителите, съхраняващи информацията, така и на крайните потребители.

Конфиденциалността на информацията е от особено голяма важност, когато се отнася до личните данни на служители, клиенти или пациенти. Всички, които контактуват с дадена организация, очакват предоставената от тях информация с лични данни, да бъде строго конфиденциална. Понякога разкриването ѝ е преднамерено, а в други случаи това може да стане случайно. Например, когато конфиденциална информация по грешка се изпрати на потребител извън организацията или когато служител изхвърли документ, съдържащ важни данни без да го унищожи.

Интегритет/Цялостност

Интегритетът на информацията е застрашен когато е обект на повреда, разрушаване или нарушаване на автентично ѝ състояние. Много компютърни вируси и червеи са създадени с ясната цел – разрушаване на данни. Поради тази причина основен метод за засичане на вирус или червей е да се провери за промени в целостта на файловете, което се констатира от техния размер. Друг ключов метод за осигуряване на целостта на информацията е **file hashing**, при който файлът се прочита с помощта на специален алгоритъм, който използва стойностите на битовете във файла за изчисление на номер, наречен **hash** стойност. Hash стойността е уникална за всяка комбинация от битове. Ако компютърната система изпълнява hash алгоритъм за файл и получава различен номер, от записаната hash стойност за този файл, то следва, че файлът е бил компрометиран и интегритетът на информацията е нарушен.

Повреждането на файловете не винаги е в резултат на външна намеса (например от хакери). Смущения в преносната среда също могат да причинят загуба на интегритет. Предаването на данни по верига с напрежение по-ниско от стандартното също може да промени или повреди данните. По време на предаването, алгоритмите, hash стойностите и кодовете за корекция на грешки осигуряват интегритета на информацията. Загубата на целостта ѝ налага нейното повторно изпращане.

Полезност

Полезността е качеството или състоянието на информацията да има стойност за постигане на определена цел. Ако информацията е налична, но не е в подходящ формат за крайния потребител, тя е безполезна.

Притежание/Владение

Притежанието на информацията е качеството или състоянието на собственост или контрол. За информацията се казва, че е собственост на даден потребител ако същият я е получил, независимо от формата или други нейни характеристики. Въпреки, че нарушаването на конфиденциалността винаги води и до нарушаване на собствеността, нарушаването на собствеността не винаги води до нарушаване на конфиденциалността. Например, ако дадена компания съхранява важни данни за клиенти с използване на криптирана файлова система и напускащ служител копира записите с цел продажбата им на конкуренти. Преместването на записите от тяхната защитена среда е нарушаване на собствеността.

КОМПОНЕНТИ НА ИНФОРМАЦИОННАТА СИСТЕМА

Информационната система (ИС) представлява съвкупност от софтуер, хардуер, данни, персонал, процедури и мрежи, които правят възможно използването на информационните ресурси в организацията. Тези шест критични компонента позволяват информацията да бъде въвеждана, обработвана, извеждана и съхранявана. Всеки от тях има своите предимства и недостатъци, характеристики и приложения. От друга страна самите компоненти на ИС също имат свои изисквания за сигурност.

Софтуер

Компонентът *софтуер* на една ИС обхваща приложения, операционни системи и различни командни средства за управление. Софтуерът е най-сложния компонент на ИС що се отнася до сигурността. Грешките в софтуера представляват една от основните заплахи за информацията.

Софтуерът е жизненоважен елемент за съхраняваната в дадена организация информация. За съжаление софтуерните продукти често се създават в рамките на ограничения на проектите – време средства, и работна ръка. За информационната сигурност се мисли в последствие, вместо да е заложена като приоритет в самото начало. По този начин софтуерните продукти стават лесна мишена за случайни или преднамерени атаки.

Хардуер

Хардуерът е физическата технология, на която се поставя и изпълнява софтуера, съхраняват и предават данни и която осигурява интерфейс за въвеждане и премахване на информация от системата. Политиките за физическа сигурност третират хардуера като физически актив и са насочени към предпазването му от увреждане или кражба.

Данни

Данните, които се съхраняват, обработват и предават чрез компютърните системи също трябва да бъдат защитени. Често те са най-ценните активи, които дадена организация притежава и са основна цел на предумишлени атаки.

Хора

Въпреки, че често се пренебрегват в съображенията за компютърната сигурност, хората винаги представляват заплаха за нея. Освен ако политиките, обучението и преподаването, запознаването с технологиите, не са създадени за предпазване от инцидентна или преднамерена повреда или загуба на информация, хората винаги ще представляват слабото звено. В този аспект социалното инженерство може да се използва за манипулиране дейностите на хората за получаване на достъп до специализираната информация за дадена система.

Процедури

Друг много често пренебрегван компонент на ИС са процедурите. Процедурите представляват писмени инструкции за изпълнение на специфични задачи. Когато неавторизиран потребител узнае процедурите на организацията, това представлява заплаха за интегритета на информацията.

Мрежи

Компонентът на ИС, който има най-голяма необходимост от компютърна и информационна сигурност е мрежата. Когато ИС се свързват една с друга за формиране на локални мрежи, а от друга страна тези мрежи са свързани с други такива, например Интернет, възникват нови предизвикателства за сигурността. Физическата технология, която позволява мрежите да функционират става все по-достъпна за организации от всякакъв ранг. Използването на традиционни средства за физическа сигурност (брави и ключове, ограничаване на достъпа до хардуерните компоненти на информационната система и взаимодействието с тях) са особено важни. Но когато компютърните системи са свързани в мрежа, само тези подходи не са достатъчни. Мерките за осигуряване на мрежова сигурност са толкова необходими, колкото и използването на системи за алармиране и проникване, които да известяват потребителя за съществуващи заплахи.

КЛЮЧОВИ ПОНЯТИЯ СВЪРЗАНИ С ИНФОРМАЦИОННАТА СИГУРНОСТ

Основните термини и понятия, важни за информационна сигурност са [2]:

- **Достъп**: възможността на субект или обект за използване, манипулиране, промяна или въздействие върху друг обект или субект. Авторизираният

потребител има легален достъп до системата, докато зложелателите имат нелегален достъп. Контролът на достъпа управлява тази възможност.

- **Актив**: това са ресурсите на организацията, които ще бъдат защитавани. Активите могат да са логически (уеб сайт, информация или данни) или физически (човек, компютърна система или др. материални обекти). Активите и особено информационните активи са обект на усилията за осигуряване на сигурност; те са тези, заради които се прилагат мерки и усилия за защита.
- **Атака**: преднамерено или непреднамерено действие, което може да причини повреда или да компрометира информацията, която системата осигурява. Атаките могат да бъдат активни и пасивни, умишлени или случайни, директни и индиректни. Човек, който случайно прочита чувствителна информация, непредназначена за него, извършва пасивна атака. Зложелател, който опитва да проникне в информационна система извършва преднамерена атака. Светкавица може да причини пожар в сградата – това е непреднамерена атака. Директна атака извършва зложелател, който използва личния си компютър за навлизане в система. Индиректна атака е тази, при която зложелател компрометира системата и я използва за атакуване на други системи.
- **Контрол, защита или противодействие**: механизми за сигурност, политики или процедури, които могат успешно да противодействат на атаки, да намаляват риска, да намаляват уязвимости и да подобряват сигурността на организацията като цяло.
- **Използване/Експлоатиране**: техника, която се използва за компрометиране (излагане на риск) на система. Зложелатели/агенти на заплахи може да опитат нелегално да експлоатират система или друг информационен актив за собствена изгода. Експлоатирането може да бъде процес за възползване от уязвимост или излагане на опасност, обикновено в софтуера. При експлоатирането се използват съществуващи софтуерни средства или специално създадени софтуерни компоненти.
- **Излагане**: условие или състояние на излагане на системата на опасност. В информационната сигурност излагане на опасност е налице когато има уязвимост, известна и на зложелателя.
- **Загуба**: информационен актив, който е бил обект на повреда, непреднамерена или незаконна промяна или разкриване. При кражба на информация, организацията претърпява загуба.
- **Защитен профил или състояние на сигурност**: цялата съвкупност от контрол и защитни мерки, включващи политики, обучение, преподаване и осведомяване, и технологии, които организацията предприема (или не успява да предприеме) за защита на активите.
- **Риск**: възможност за осъществяване на нежелани действия. Организациите трябва да сведат до минимум риска, така, че той да съвпада със степента им на възможност за неговото поемане.
- **Субекти и обекти**: компютърът може да бъде субект на атака – средство за извършване на атака – или обект на атака – цел.
- **Заплаха**: категория от обекти, които представляват заплаха за даден актив. Заплахите могат да са целенасочени или нецеленасочени. Например, зложелателите целенасочено заплашват незащитените информационни системи, докато природните стихии непреднамерено заплашват сградите и тяхното съдържание.
- **Агент на заплахи/Зложелател**: конкретна заплаха или компонент от нея.

- **Уязвимост**: слабости или грешки в система или защитен механизъм, които предразполагат към атака или повреда. Примери за уязвимости са недостатък в софтуера, незащитен системен порт и др.

ЗАКЛЮЧЕНИЕ

Настоящият документ е изготвен с финансовата помощ на Европейския социален фонд. Русенският университет „Ангел Кънчев" носи цялата отговорност за съдържанието на настоящия документ, и при никакви обстоятелства не може да се приеме като официална позиция на Европейския съюз или Министерството на образованието и науката". Проект:№ BG051PO001-3.3.06-0008 „Подпомагане израстването на научните кадри в инженерните науки и информационните технологии. Публикацията разглежда същността на информационната сигурност, основните компоненти на информационните системи, важни характеристики на информацията и ключови понятия, свързани с нейната сигурност.

ЛИТЕРАТУРА

[1] Easttom, Ch. Computer Security Fundamentals. Copyright Pearson, 2012, 350p.
[2] Vacca, J. Managing Information Security. ELSEVIER Inc., 2010, 321p.
[3] Whitman, M., H. Mattord. Principles of Information Security, Course Technology, Cengage Learning, 2012, 658p.

За контакти:

Доц. д-р Валентина Войноховска, Катедра *Информатика и информационни технологии*, Русенски университет *Ангел Кънчев*, тел.: 082-888 645, e-mail: voinohovska@ami-uni.ru.acad.bg

Гл. ас. д-р Светлозар Цанков, Катедра *Информатика и информационни технологии*, Русенски университет *Ангел Кънчев*, тел.: 082-888 645, e-mail: stzancov@ami.uni-ruse.bg