СИГУРНОСТТА В СЪВРЕМЕННИЯ ВИРТУАЛЕН СВЯТ

Пеньо ГЕОРГИЕВ*

In the present work, the author presents the hazards surrounding our most valuable resource, namely information. The world that we have known for a long time has evolved imperceptibly, and we have sunk into virtual existence, surrounded by the technologies and techniques that govern us, our documents, our data and our everyday life. Information as a resource is more and more easily accessible, although it has a personal, secret, corporate character, or a national security status. In view of the above, it is good to build ways and algorithms to prevent various attacks in the virtual world, but also to educate people about basic hygiene in dealing with risky information resources, technologies, software applications, and more.

Увод

Липсата на задълбочено обучение в неспециализираните висши училища по тази тематика е предпоставка за пренебрежението на аспекта сигурност на нормалните потребители на различни информационни системи.

Ползата от внедряване на информационните технологии в живота на съвременното общество е повече от видима, което предполага силната нужда от решения на редица информационни проблеми, свързани с информационната безопасност. Гарантирането на безопасност в различните информационни системи може да се различава съществено, но то винаги е насочено към това да се достигнат три основни свойства: цялостност (информация, на основата на която се приемат решения, трябва да бъде достоверна и точна, защитена от възможно неумишлено и умишлено изопачаване), достъпност (информацията и съответните автоматизирани служби трябва да бъдат достъпни, готови за работа винаги когато възникне необходимост) и конфиденциалност (засекретената информация трябва да бъде достъпна само за този, за когото е предназначена).

Информацията като ресурс е един от най-мощните за икономическо развитие. Притежаването и използването на конкретна информация в

* Авторът е асистент, доктор, Пловдивски университет „Паисий Хилендарски".

определено време за конкретни цели са предпоставка за успех на всеки. Притежанието на информационни масиви определя субекта с по-добър показател спрямо другите, или с други думи придобива предимство пред останалите. В съвременната обстановка фирмите са закъснели, ако не са въвели информационни системи, подпомагащи управлението им. Дори и при малките и средни предприятия се наблюдава ръст на използването на софтуери за специфични нужди. Всички тези интегрирани системи генерират огромен обем от информация в локалните мрежи на предприятията, в техните работни компютърни станции и извън техните мрежи, предавани чрез интернет. Точно тези информационни масиви са предмет на злонамерени действия. Рано или късно се появява момент, в който е причинено проникване, загуба, промяна, подмяна или друго действие с определен информационен ресурс, което е довело до малки или в повечето случаи до огромни загуби на организацията, обикновено финансови.

Съществуват много видове зловреден софтуер, появяват се непрекъснато нови вируси, нови алгоритми за заблуда и други способи за нанасяне на вреди. Битката водим на различни нива, едно от които е: добре е да сме в крак с последните новости, или да сме „up to date“.

В следващите точки се представят познати видове вируси, зловреден софтуер, как възникват, как разпространяват нанесените от тях вреди и как можем да се предпазим.

Заплахи и опасности

Революцията в технологиите и в комуникациите коренно промени света, в който живеем. Информационните технологии промениха из основи естеството на междуличностните взаимодействия. Интернет свърза общества от всички краища на Земята. Социалните мрежи позволяват на всеки индивид да споделя информация навсякъде по Земното кълбо за секунди. А глобалната мрежа ни предлага дигитално хранилище, в което всеки може да запази срещу минимално или без никакво заплащане лична или професионална информация [1].

Представата на потребителите за виртуалното пространство често дори ни най-малко не се доближава до многомерността на виртуалния свят. Представата им е илюзорна за това, че той е огледален образ на реалния свят. Заплахите са невидими, неочаквани и мигновени, а опасностите се крият дори в най-безобидния на пръв поглед файл. Авторът смята, че е редно да се отбележат някои от познатите опасности и да се предложат добри практики за реакция и превенция.

Информационна сигурност

Информационната сигурност [5; 7] може да бъде представена като различни аспекти, които могат да засягат информационните ресурси физи-

чески – пряко, целенасочено или неумишлено, както и виртуални посегателства. Някои от най-често срещаните и познати заплахи и опасности са:

1) Физическа сигурност на компютърните системи – *Кражба или неоторизиран физически достъп; Природни стихии, технически сривове поради повреда или външни технически обстоятелства.*

2) Заплахи от собствения персонал – *Неволни технически грешки; Други грешки и социално инженерство; Злонамерени служители.*

3) Злонамерени действия от външни лица – *Хакери и кракери; Неоторизиран достъп чрез пароли.*

4) Phishing

5) Вреден софтуер (вируси) – *Резидентни; Boot; Вируси с директно действие; Stealth; Макровируси; Логически вируси; Time-bomb; MBR (Master Boot Record); BIOS вируси; Размножаващи се; Joke programs; Virus creating tool viruses; Хардуерни вируси; Суматорни вируси; Псевдорутерни; Информационни замърсители; Полиморфни вируси; Биокомпютърни вируси; Бинарни вируси; RAM вируси; Companion вируси; Вируси убийци; FAT Scrabmlers; Java вируси; E-mail вируси; WAP вируси; Червеи (Worms); Host червеи; Net Worm; Троянски кон; „Терористи“ (Droppers); Бомби; INI програми; BAT инфектори; Задна врата (Backdoor); Шпионски софтуер (Spyware); Рекламен софтуер (Adware); Програми за запис на клавиши/работен плот (Keystroke logging/Screen logging); Фалшив софтуер (Rogue); Руутким (Rootkit).*

6) Кражба на самоличност

7) Паролите не са толкова сигурни

8) Паролите са неудобни

Сигурност или хигиена на „сърфирането“ във виртуалния свят

Сигурността на информацията [2] като стратегически важен ресурс изисква тя да бъде защитена от създаването до нейното унищожаване. Защитата е добре да бъде на всички нива – от най-ниското хардуерно или на ниво мрежова сигурност [6] до защитата на самите данни. Информацията може да се класифицира най-общо като Публична информация или Служебна информация, също така може и да бъде Конфиденциална информация. От гореизложеното ясно се вижда необходимостта от въвеждане на стандарти за системи за управление на сигурността на информацията. Такива действащи стандарти могат да бъдат закупени от Българския институт по стандартизация (БИС) [8]. Всички внедрени системи и правила би следвало да не противоречат на законите и нормативните актове в Република България.

Нормативни актове

1) Закон за защита на класифицираната информация – ДВ, бр. 45/2002.

2) Закон за защита на личните данни – ДВ, бр. 1/2002.

3) Наредба за задължителните общи условия за сигурност на автоматизираните информационни системи/мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация – ПМС № 99/10.05.2003, ДВ, бр. 46/2003.

4) Наредба за криптографска сигурност на класифицираната информация – ДВ, бр. 102/21.11.2003.

5) Правилник за прилагане на Закона за защита на класифицираната информация – ПМС № 276/2.12.2002, ДВ, бр. 115/10.12.2002.

6) Доктрина за комуникационните и информационни системи на БА, 2001 – приета от Съвета по отбрана, Протокол № 4/4.03.1999.

7) Концепция за информационна стратегия на МО – приета от Съвета по отбрана, Протокол № 6/20.04.1999.

8) Концепция за информационна дейност на МВР – ДВ, бр. 38/30.04.2001.

Стандарти на БИС

1) БДС ISO/IEC 27000:2016 – Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Общ преглед и речник *(БДС ISO/IEC 27000:2016 заменя и отменя БДС ISO/IEC 27000:2014 на 2016-03-17)*

2) БДС ISO/IEC 27001:2013/Cor. 1:2016 – Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания. Техническа поправка 1

3) БДС ISO/IEC 27001:2013/Cor. 2:2016 – Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания. Техническа поправка 2

4) БДС ISO/IEC 27001:2014 – Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания *(БДС ISO/IEC 27001:2014 заменя и отменя БДС ISO/IEC 27001:2006 на 2014-05-19)*

5) БДС ISO/IEC 27003:2011 – Информационни технологии. Методи за сигурност. Указания за внедряване на системи за управление на сигурността на информацията

В специализирания сайт на БИС могат да се намерят и други стандарти за системи за управление на сигурността на информацията, но те са със статут отменен.

Правила на хигиена, които да спазваме

Разбираемо е, че не може да бъде определено и няма такова универсално решение, което да предпази, да защити абсолютно дадена информация. Няма такъв способ или софтуерно приложение, което да осигури 100-процентова защита, и е немислимо да се търси такова решение,

като се има предвид разнородният и необхватен виртуален свят. Съществуват и виртуални пространства, които са с осигурена защита, понеже те са с контролирани точки за достъп. Такова пространство е Виртуалното образователно пространство (ВОП) [3].

Авторът смята за добър варианта, в който управленските нива на организациите прилагат или гореизложените стандарти, или практики и процедури, съобразени с тяхната дейност. Обръща се внимание на организацията на фирмените информационни системи, на тяхната защита [4] и на обучението на служителите, като последното е редно да бъде застъпено по-широко във висшите училища.

Мерки за налагане на информационна сигурност

1) Административни (организационни, процедурни) мерки
2) Логически (технически) мерки
3) Физически мерки
4) Управленски мерки
5) Контрол на достъпа – Автентикация – адаптивна автентикация; смарт карти; телефонна автентикация; биометрична автентикация и др.

Процедури за сигурност

1) Физическа сигурност
2) Персонална сигурност
3) Документална сигурност
4) Маркиране и отчет на класифицирана информация в АИС или мрежи
5) Регистриране, маркиране, отчет и унищожаване на материални носители за многократен запис на класифицирана информация
6) Комуникационна и криптографска сигурност, защита от паразитни електромагнитни излъчвания
7) Минимални изисквания за компютърна сигурност
8) Режими на сигурност
9) Сигурност по време на експлоатацията и развитието на сертифицирани АИС или мрежи
10) Сигурност на АИС или мрежи, в които се създава, обработва, съхранява или пренася информация с класификационно ниво „Строго секретно“
11) Възможност за заместване на мерките за компютърна сигурност

Сигурност в компютърните системи и мрежи с достъп до интернет

1) Надеждност на информацията
2) Проверка за вируси
3) Технологии за автоматично обновяване

4) Spoof на потребители
5) Анонимност на потребителя
6) Java
7) Промяна на уебстраници

Технически способи за защита

1) Криптография
2) Екраниране
3) Използване на терминали
4) Използване на непрекъсваемо електрозахранване

Препоръки за потребители

1) Включете Data Execution Prevention (DEP)
2) Не спирайте User Account Control (UAC) под Windows
3) Замислете се да преминете под стандартен/ограничен акаунт
4) Не изключвайте вградената защитна стена в Windows
5) Поддържайте софтуера си актуален
6) Спрете функцията за автоматично изпълнение (auto play) в Windows
7) Не се размотавайте из съмнителни сайтове и P2P мрежи и не сваляйте кракове за програми
8) Използвайте допълнителен защитен софтуер
9) Внимавайте за различни видеофайлове и онлайн клипове, които изискват специфичен кодек, за да се възпроизвеждат
10) Внимавайте за спам съобщения в месинджърите, които използвате (особено Skype)
11) Ползвайте Facebook по-кротко/по-малко или въобще не го ползвайте
12) Сваляйте програми само от надеждни източници
13) Поддържайте актуален образ на системния дял
14) Поддържайте сигурност на паролите
15) Изпълнявайте криптиране на файлове
16) Включете протоколът IP Security
17) Изисквайте Secure Sockets Layer (SSL) при уебтрансакции
18) Изисквайте сигурност на електронната поща
19) Използвайте антивирусни програми
20) Не използвайте публични Wi-Fi мрежи без защитена връзка (VPN)

Заключение

Редом с реалните заплахи от реалния сват все повече ставаме свидетели на опасности, произлизащи от заобикалящите ни компютри, мобилни устройства, интернет, които са не по-малко опасни. Превенцията

на този тип заплахи трябва да бъде системна, последователна, с ясно разписани правила и цели. Добре е да има единна стратегия за реагиране и превенция при виртуални заплахи, още повече такава е задължителна в големите корпорации, а вече и в малките и средните предприятия, стигайки до самия потребител и неговите лични данни. Основните заплахи за информацията са известни: вреден софтуер, нелоялни служители, човешка грешка, техническа неизправност, външни атаки и др. Авторът смята за необходимо изготвянето на стратегии и тактически планове за защита на информацията в МСП и личните данни, поради което ще засили изследването на проблемната област.

Литература

1. **Арнаудов,** Д., А. Крумова. Сигурност и защита на информационните системи. Варна: Черноризец Храбър, 2007.
2. **Савов,** И. The Collision of national security and Privacy in the Age of Information Technologies. – In: *CEPOL* – European Police Science and Research Bulletin, issue 15, 2016.
3. **Семерджиев,** Ц. Информационна сигурност. София: Софттрейд, 2004.
4. **Семерджиев,** Ц. Сигурност и защита на информацията. София: Класика и стил, 2007.
5. **Станев,** С., С. Железов. Компютърна и мрежова сигурност. Шумен: Епископ Константин Преславски, 2005.
6. **Стоянов,** С. Теоретичен модел на виртуално образователно пространство. – В: *Международна* конференция „From DeLC to VelSpace“, 26 – 28 март, Пловдив, с. 285 – 297.
7. *http://www.tuj.asenevtsi.com/Sec2009/Sec01.htm*
8. *http://www.bds-bg.org*