ПРАКТИЧЕСКА КИБЕРСИГУРНОСТ ЗА МАЛКИТЕ И СРЕДНИТЕ ПРЕДПРИЯТИЯ

Пеньо ГЕОРГИЕВ*

This paper presents practical examples of cyber security policies for small and medium-sized businesses. The security of small and medium-sized enterprises plays an important role in national security. The goal is to bring a simplified cyber security model for micro enterprises in the context of the National Cyber Security Strategy „Cyber Resilient Bulgaria 2020".

Увод

В следващите редове на този материал ще се представят полезни практически примери за защита на информационните ресурси на малките и средните предприятия (МСП). Като основна част от българската икономика сигурността на МСП играе важна роля за националната сигурност. В този смисъл може да се каже, че националната сигурност включва в себе си и сигурността на малките и средните предприятия. Разглеждането на полезни примери и модели касае аспекта на киберсигурността на МСП.

Защо е важно да се търсят модели и решения за защита на МСП?

– Повечето МСП не разполагат с ресурси за осигуряване на защита на информационните си системи.

– Не разполагат с обучени специалисти.

– Не познават добре заплахите и техните аспекти.

– Не познават рисковете и последиците от различни злонамерени действия.

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

Гореизложеното дава възможност да се търсят подходящи практики, които лесно да могат да се внедрят както в МСП, така и във всяко домакинство или за лична употреба.

„В България близо 60 % от домакинствата и над 90 % от предприятията имат достъп до интернет, като 50 % от предприятията използват автоматизиран обмен на данни с външни ИКТ системи. Почти цялата комуникация на публичната администрация с бизнеса е само електронна, нарастват и услугите към гражданите, които се извършват предимно по интернет. Интернет свързаността и скоростта на информационните канали непрекъснато расте – България е в групата на Топ 20 в света по скоростен интернет и между първите по степен на въвеждане на високоскоростен, което предоставя нови възможности за отдалечени и облачни услуги, но и нови възможности за мащабно и злонамерено използване“ [1].

Бързото развитие на съвременните информационни технологии, широкото внедряване на цифрови средства за видео- и аудиозапис, за фотоснимки и мобилна комуникация доведоха до това, че разследващите служители в последно време постоянно се сблъскват с нова среда за извършване на престъпления – киберпространството, образувано от носителите на компютърна информация, представена в дискретен вид [2].

Картината, която се формира, е почти масово използване на интернет от всички в страната. Както достъпът е двупосочен за всички, които ползват определени услуги или информационни мрежи, така и пътят към тях е отворен за злонамерени и опасни действия.

Търси се опростен модел или конкретни правила, които да повишат нивото на защита или поне да ограничат в известна степен най-често използваните атаки.

Разглеждат се следните съвети за киберсигурност, които се предлагат от Федералната комисия по комуникациите на САЩ [4]:

Обучение на служителите по принципите на сигурността

Обучението на служители е важен процес. Той е непрекъснат и периодичен.

– Документиране на политиките за киберсигурност.

– Периодично провеждане на обучение на всички служители по внедрените политики и процедури.

Разработването на такива политики и процедури е непосилна задача за едно малко предприятие. Предлага се използването на вече утвърдени практики, като:

- БДС EN ISO/IEC 27000:2017 [5];
- БДС EN ISO/IEC 27001:2017 [6]
  - Информационни технологии;
  - Методи за сигурност;
  - Системи за управление на сигурността на информацията.

Не бива да се пропуска и детайлното разглеждане на **GDRP** [6], когато дейността на МСП попада в обхвата на регламента. Защитата на личните данни е ясно дефинирана, а полезни насоки могат да се получат от **Комисията за защита на личните данни,** *„Десет практически стъпки за прилагане на общия регламент относно защитата на данните“* [8].

В контекста на борбата с тероризма развитието на телекомуникациите и възходът на дигиталните технологии предизвикаха безпрецедентни предизвикателства в защитата на неприкосновеността и личната информация [3].

ЗАЩИТЕТЕ ИНФОРМАЦИЯТА, КОМПЮТРИТЕ И МРЕЖИТЕ ОТ КИБЕРАТАКИ

Първата точка разглежда определянето и внедряването на политиките и процедурите за сигурност. В тази точка би следвало да приложим на практика способи за защита на зоните, в които попадаме.

- Защитата посредством **антивирусен софтуер** е възможно най-минималното ниво, което трябва да съществува. Авторът предлага следния подход: *„Ако имате едно ниво на защита – нямате защита, ако имате две нива на защита – имате слаба до добра защита, и ако имате най-малко три нива – тогава имате повече от добра защита“.*

- Важно е да се следят и последните обновления на операционните системи и приложния софтуер и да се поставят поправките в сигурността.

- Контролът върху мрежата да е установен и достъпът до ресурсите да става спрямо определена процедура.

- Криптирането на информацията е важен момент от самата ѝ защита.

- Добре е да се определи отговорник по сигурността (кибер-сигурността).

Това са практически критични изисквания към системата за сигурност. От гледна точка на разглежданата област авторът се опитва да представи минималистичен опростен модел за базисна защита на едно МСП. В по-горните описани стандарти и регламент е оформена представа за детайлната рамка на една система за сигурност.

ОСИГУРЕТЕ ЗАЩИТНА СТЕНА ЗА ВАШАТА ИНТЕРНЕТ ВРЪЗКА

В тази точка се акцентира на защитата в етап на входящия трафик на интернет и неговото филтриране посредством защитни стени. Внедряването на такива защитни стени се пренебрегва почти винаги от МСП поради факта, че не се осъзнава тяхното значение, нелеката им настройка и нуждата от експертни познания. Авторът смята, че тази точка е важна и не бива да се пропуска като модул от цялата информационна система. Могат да бъдат внедрени и облачни услуги, чрез които да се управляват трафикът от трети лица. Едни от водещите компании в света, като **Fortinet** и **Cisco,** предлагат най-високо ниво на защита. Моделите, които разработват, предоставят и следващо поколение интелигентни защитни стени и способи за прихващане на аномалии и зловредни процеси. Ако се приеме, че е налице невъзможност за поставяне на такава защитна стена, то тогава най-малко трябва да бъде предвидена настройка на правила в защитната стена на операционната система или антивирусният софтуер да разполага с такъв модул.

СЪЗДАЙТЕ ПЛАН ЗА ДЕЙСТВИЕ ЗА МОБИЛНО УСТРОЙСТВО

Всички сме свикнали да оперираме с мобилни устройства и сякаш са неразделна и естествена част от живота ни. В този смисъл не определяме мобилните устройства като явна заплаха, а те могат да се превърнат в точка за достъп до вътрешната ни мрежа и да застрашат сигурността на системите ни. За да се избегнат такива мероприятия, авторът предлага стриктен контрол на мобилните устройства като неразделна част от комуникационната система.

Такъв контрол следва да е определен в процедурите от първа точка. Примерни процедури:

- управление на преносими носители;
- унищожаване на носители.

Процесът на унищожаване на носители на информация, включително и на твърди дискове, които няма да бъдат използвани повече от организацията, се свежда до следните стъпки. Управителят преценява кой е подходящият метод за унищожаване за конкретен носител (в зависимост от това дали той ще продължава да се ползва, или ще се извежда от употреба), а именно:

- изтриване – действие, при което само се премахва директория или каталожна връзка към информацията. В действителност файловете продължават да съществуват върху носителя.
- демагнитизиране – действие, при което магнитният носител се възстановява до състоянието, преди да бъде използван.
- физическо унищожаване – действие, при което носителят се унищожава физически до степен, непозволяваща възстановяване на информация от него, например изгаряне, надробяване на малки късчета или друг подходящ начин, позволяващ физическото разрушаване на носителя и невъзможността за следващо изтичане на информация.
- транспортиране на носителя.

НАПРАВЕТЕ РЕЗЕРВНИ КОПИЯ НА ВАЖНИ БИЗНЕС ДАННИ И ИНФОРМАЦИЯ

Резервирането и архивирането на критична информация е често пропускана процедура. Настройката на периодични резервни копия не е сложна и трудоемка операция. Тук е възможно за целта да се използват както самите операционни системи, така и допълнителни специализирани приложни софтуери. Възможни са централизирани решения, както и разпределени към крайния потребител. Примери на водещи компании в разработването на такъв тип приложен софтуер:

- Acronis True Image 2019;
- EaseUS ToDo Backup;
- Paragon Backup & Recover Advanced;
- NovaBackup PC;
- и др.

Контролирайте физическия достъп до компютрите си и създайте потребителски акаунти за всеки служител

Определянето на физическия достъп е достатъчно сложна задача. Авторът предлага няколко примерни добри практики да бъдат заложени като процедури в изграждането на системата за сигурност:

- Граници на физическата сигурност
- Механизми за контрол на физическата сигурност
- Осигуряване на офиси и съоръжения
- **Разполагане и защита на оборудването:**

o Критичното оборудване се поставя в специализирани помещения, така че да се намали до минимум неоторизираният достъп до него;

o Условията на окръжаващата среда, и по-конкретно температура и влажността, са наблюдавани и контролирани от климатизационни системи, с което се избягват неблагоприятни работни условия на средствата за обработка на информация;

o Сървърите и цялото мрежово оборудване следва да са осигурени с непрекъсваеми токозахранващи източници със съответния капацитет, поддържащи оборудването за поне 15 мин. от отпадане на елзахранването;

o Оборудването на локалната мрежа трябва да е обезопасено чрез монтиране в специализирани комуникационни шкафове или кутии със заключваща се врата;

o Защитата срещу неоторизиран достъп до хардуерни компоненти на критичното оборудване се осигурява чрез разрушаващи се при отваряне – залепващи ленти.

- Сигурност на окабеляването
- Поддръжка на устройствата
- и др.

Създаването на потребителските акаунти за достъп ще се разгледат подробно в точка 8.

Защитете Wi-Fi мрежите

Безжичните мрежи са едни от най-лесните за пробив звена в цялостната мрежова архитектура на фирмената мрежа. Често се поставят точки за достъп, директно свързани, без да се направят

дори минимални усилия за защитата им, което от своя страна предоставя лесен достъп за атаки. Примери за защита на безжични мрежи.

При наличието на рутер, предоставящ достъп до вътрешната мрежа и мрежата за гости, тогава:

- е необходимо да се вземат всички необходими мерки за забраната на всякакъв вид свързаност между безжичната мрежа за гости и служебната кабелна или безжична мрежа;
- безжичната мрежа за гости не трябва да дава достъп до нито един от ресурсите на фирмата – тя трябва да дава достъп само до интернет;
- администрирането на рутерите се извършва с комплексни пароли за достъп с поне 12 символа, които се сменят на всеки три месеца;
- достъпът до безжичните мрежи се конфигурира с комплексни пароли за достъп с поне 12 символа, които се сменят на всеки три месеца;
- връзката през безжичния рутер се осъществява посредством WPA2 криптиране.

Ограничете достъпа на служителите

Политика за контрол на достъпа. Политиката за контрол на достъпа има за цел да регламентира трансфера на информация от пасивния обект на достъп (информационна система, база данни, приложение, файл и т.н.) към активния субект (потребител, информационна система, приложение и т.н.), заявяващ достъпа.

- Достъп до мрежи и мрежови устройства
- Регистрация и дерегистрация на потребителите
- Обезпечаване на правата на потребителите

o За нуждите на идентификацията всеки потребител ползва уникално потребителско име или идентификатор. Общи (споделени) акаунти не са позволени.

o За нуждите на идентификацията, т.е. проверката на идентичността, се прилага класическият метод за това чрез пароли. Допълнително за някои ресурси може да се изисква и допълнителна автентификация чрез цифров сертификат или ключ.

o Достъпът се осигурява чрез домейн контролер. За целите на контрола на достъпа са налични политики на домейн контролера.

- управление на привилегировани права за достъп
- принципи при избор на парола
- процедура за сигурно влизане в системата (secure log-on)
- система за управление на паролите
- и др.

Пароли и удостоверяване

- Прилагайте практики за безопасна парола. Паролите трябва:

o да съдържат малки и главни букви (например: a – z, A – Z);

o да ъдържат цифри и пунктуационни символи, а също така и букви (например: 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./);

o да са не по-малко от 8-буквени – цифрова и символна комбинация за пароли на локални потребители и потребителски акаунти в системи, достъпни само от вътрешната компютърна мрежа на организацията (включително хардуерно изградената виртуална частна мрежа между офисите), и най-малко 12-буквени – цифрова и символна комбинация за администраторски пароли на сървъри и маршрутизатори, уеббазирани системи и пароли за VPN достъп. Потребителските пароли за достъп до достъпни от публична мрежа уеббазирани системи трябва да бъдат минимум 8-символни, комплексни (малки и главни букви, цифри и специални символи);

o да не се базират на лична информация, имена на роднини, ЕГН и т.н.;

o да не се записват или съхраняват; опитайте се да създавате пароли, които можете да запомните;

o да не се повтарят със стара такава в рамките на последните 5 промени;

- Използвайте многофакторна идентификация.

Заключение

В по-горе изложеното авторът има за цел в бъдещите си разработки да изгради представа за единен опростен модел на сигурност, който да бъде лесноприложим в МСП. Тази цел е поставена в контекста на Националната стратегия за киберсигурност „Киберустойчива България 2020". Очакваният резултат от прилагането на изброените по-горе процедури е да бъдат покрити нивата „Информационна сигурност" и „Киберсигурност" на *Фигура 1* [1].

Фигура 1. *Нива на сигурност*

Литература

1. **Костов,** Д. Световната икономика и новият икономически ред. София: Албатрос, 2017. ISBN 978-954-751127-9.

2. **Национална** стратегия за киберсигурност „Киберустойчива България 2020“.

3. **Савов,** И. Един поглед върху същността на киберпрестъпността. – В: *Политика* и сигурност, ВУСИ, 2017, с. 36 – 47. ISSN 2535-0358.

4. **Савов,** И. Един поглед върху неприкосновеността и защитата на личните данни в дигиталната ера. – В: *Бюлетин,* бр. 37, Факултет „Полиция“, Академия на МВР, 2017, с. 79 – 97. ISSN 1312-6679.

5. *https://www.fcc.gov/general/cybersecurity-small-business.* [прегледан 3.03.2019 г.].

6. *http://www.bds-bg.org/bg/standard/?natstandard_document_id=82280.* [прегледан 3.03.2019 г.].

7. *http://www.bds-bg.org/bg/standard/?natstandard_document_id=82281.* [прегледан 3.03.2019 г.].

8. *https://www.cpdp.bg/userfiles/file/New_legislation/Regulation_EU_2016_679_Bg.pdf.* [прегледан 3.03.2019 г.].

9. *https://www.cpdp.bg/?p=element&aid=1109.* [прегледан 3.03.2019 г.].