7. ECONOMIC SECURITY OF BUSINESS ENTITIES

Bashynskaya I.
PhD in economic sciences
Odessa national polytechnic university

INFORMING STAFF AND COMPANY MANAGMENT ABOUT THREATS AND RISKS OF INFORMATION SECURITY

Башинська І.О.
к.е.н.
Одеський національний політехнічний університет

ІНФОРМУВАННЯ ПЕРСОНАЛУ ТА КЕРІВНИКІВ ПІДПРИЄМСТВА ПРО ЗАГРОЗИ ТА РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

In the article the need of informing company personnel about possible threats and information security risks is considered. The algorithm of information is proposed. It consists of 2 stages: the first stage – preparation employees to possible threats; second stage – creating the official program management of mobile devices.

Key words: *information security, information, mobile devices, phishing, cyber threats, security breach, cyber attacks.*

Розглянута необхідність інформування персоналу підприємства про можливі загрози та ризики інформаційної безпеки. Запропоновано алгоритм інформування, який складається з 2-х етапів: перший етап - підготовка службовців до можливих загроз; другий етап: створення офіційної програми управління мобільними пристроями.

Ключові слова: *інформаційна безпека, інформування, мобільні пристрої, фішинг, кіберзагрози, порушення захисту, комп'ютерні атаки.*

На сьогоднішній день інформаційна сфера є ведучою в діяльності держави і чинить вплив на всі елементи функціонування підприємств. Разом зі зростаючою залежністю від електронних технологій, пов'язаних з поширенням інформації, зростає і загроза кібератак, метою, яких, як правило, стають інформаційні ресурси та мережева інфраструктура [1]. Головна задача інформаційної безпеки (кінцевий результат) полягає у вирішенні інформаційно-аналітичними засобами не тільки проблем захисту від загроз, що виникають, а, перш за все, завчасне розкриття і попередження суб'єкта управління про причини і умови, які можуть сприяти виникненню ранніх ознак цих загроз , а саме: ризиків, небезпек і викликів.

Розмір організації ніяк не впливає на необхідність захисту належної їй інформації. В умовах інформатизації особливу небезпеку представляють такі способи несанкціонованого доступу до конфіденційної інформації, як копіювання, підробка, знищення [2].

Копіювання. При несанкціонованому доступі до конфіденційної інформації копіюють:

- документи, що містять цікаву для зловмисника інформацію;
- технічні носії;
- інформацію, оброблювану в автоматизованих інформаційних системах.

Використовуються такі способи копіювання: світлокопіювання, фотокопіювання, термокопіювання, ксерокопіювання та електронне копіювання.

Підробка. В умовах конкуренції підробка, модифікація і імітація набувають більших масштабів. Зловмисники підробляють довірчі документи, що дозволяють отримати певну інформацію, письма, рахунку, бухгалтерської та фінансову документацію; підробляють ключі, пропуску, паролі, шифри і т. п. В автоматизованих інформаційних системах до підробки відносять, зокрема, такі зловмисні дії, як фальсифікація (абонент-одержувач підробляє отримане повідомлення, видаючи його за дійсне в своїх інтересах), маскування (абонент -відправник маскується під іншого абонента з метою отримання ним охоронюваних відомостей).

Знищення. Особливу небезпеку становить знищення інформації в автоматизованих базах даних і базах знань. Знищується інформація на магнітних носіях за допомогою

компактних магнітів і програмним шляхом («логічні бомби»). Значне місце у злочинах проти автоматизованих інформаційних систем займають саботаж, вибухи, руйнування, виведення з ладу з'єднувальних кабелів, систем кондиціонування.

Ключовим чинником є інформованість співробітників про проблеми IT-безпеки. Відповідно до недавнього дослідження Check Point «Звіт з безпеки 2013» (Check Point Security Report 2013) 3], у 54% з майже 900 опитаних організацій з усього світу мався хоча б один випадок потенційного витоку даних через помилкове відправлення електронних листів адресатові за межами організації або некоректної публікації інформації в Інтернеті. Також з'ясувалося, що 52% співробітників організацій ризикують допустити витік інформації через використання небезпечних методів роботи з комп'ютером.

У доповіді підкреслюється, що:

63% організацій були заражені ботами;

75% організацій відвідали шкідливі веб-сайти;

54% організацій мали принаймні один потенційний інцидент втрати даних;

36% фінансових організацій відправили інформацію про кредитну картку за межами організації;

16% з медичних і страхових організацій відправлено HIPPA-захищену інформацію про здоров'я за межами організації.

Зловмисники прагнуть скористатися саме такими простими людськими помилками: обманом змусити нічого не підозрюючого працівника перейти за посиланням у фішинговому електронному листі, який заразить його комп'ютер, або опублікувати конфіденційну інформацію на фіктивному сайті. На жаль, всіх привчили довіряти людям, і цю звичку складно змінити: співробітники організацій хочуть бути корисними і відчувати, що ефективно виконують свою роботу. Навчання співробітників допоможе підвищити їх обізнаність у питаннях безпеки.

Необхідно інформувати персонал про потенційні ризики та загрози, а також про те, як знизити ці ризики, уникаючи фішингових електронних листів, фіктивних веб-сайтів тощо. Тут у малих підприємств є перевага: їм доведеться навчати менше співробітників. Часто саме такі прості заходи дозволяють уникнути порушень безпеки.

«Кіберзагрози», «Порушення захисту», «комп'ютерні атаки». У міру поширення мобільних технологій ці слова міцно входять в наше життя. У той час, як уряди в усьому світі намагаються побудувати в рівній мірі захищену і мобільну інфраструктуру, проблема кіберзлочинності все частіше згадується у зведеннях національних новин.

Mobile Work Exchange опублікували результати самооцінки, які показують цікаву статистику, допомагаючи краще зрозуміти передові методи і слабкі сторони мобільної безпеки. Особливу увагу в звіті приділено держслужбовцям, 90% яких заявили, що використовують для роботи щонайменше один мобільний пристрій. Виявилося, що багато держслужбовців (41 %) піддають себе і свої установи ризику [4]. Ось ще деякі цікаві факти:

Мобільні пристрої:

31% користується загальнодоступним Wi-Fi-з'єднанням;

25% не встановили пароль;

6% держслужбовців, що використовують мобільний пристрій в роботі, заявили, що втрачали або забували свій телефон.

Це понад 3500 можливостей порушення захисту у федеральному агентстві середнього розміру.

Незважаючи на діючу в США федеральну стратегію електронного уряду, більше чверті з опитаних держслужбовців не проходили підготовку з мобільної безпеки в своїх установах.

Враховуючи цю інформацію, стає зрозуміло ту кількість порушень захисту, які стали темою новинних повідомлень в останні роки. Факти свідчать про те, що держслужбовці повинні переоцінити свою поведінку з точки зору мобільної безпеки, а державні установи – посилити протоколи мобільного захисту.

Враховуючи, що перехід на мобільні технології і хмарні сервіси створює значне навантаження в частині забезпечення захисту кінцевих терміналів і мобільних пристроїв, які в певних випадках можуть і не торкнутися корпоративну мережу, можливо запропонувати державним установам наступний двоетапний підхід.

Перший етап: підготовка службовців до можливих загроз.

Інформування працівників про можливі ризики та загрози при використанні власних або наданих пристроїв може надати істотну допомогу в припиненні зловмисних дій.

Бретт Белдінг (Brett Belding), старший менеджер Cisc- з питань IT-мобільності, недавно написав у своєму блозі, що така залежна від співробітників модель поведінки здатна визначити майбутнє мобільних технологій. Необхідно заохочувати діалог користувачів з IT-відділами з приводу захищеного використання мобільних пристроїв, сучасних загроз і способів їх усунення. По мірі все більшого поширення в держустановах підключених пристроїв, таких як інтелектуальні аксесуари, важливість цього завдання буде тільки рости.

Другий етап: створення офіційної програми управління мобільними пристроями.

Багатьом держустановам, особливо з обмеженим IT-бюджетом, складно управляти напливом нових типів підключених пристроїв. Щоб протистояти всіляким атакам, необхідно реагувати на величезну різноманітність векторів загроз, використовуючи рішення, що забезпечують захист за всіма напрямками (мережа, кінцеві термінали, мобільні пристрої та віртуальні середовища).

Згідно зі звітом Cisco з інформаційної безпеки за 2014 р., одне з рішень для підвищення інформаційної безпеки полягає у створенні офіційної програми управління мобільними пристроями, що забезпечує захист кожного пристрою до надання доступу до мережі. Для аутентифікації користувачів слід, принаймні, запитувати персональний ідентифікаційний код (PIN). При цьому IT-служба повинна мати можливість дистанційно відключати пристрій або прати його пам'ять у випадку втрати або крадіжки.

У своїй мобільного стратегії всі організації, і особливо держустанови, повинні прагнути до встановлення оптимального балансу довіри, прозорості та конфіденційності, оскільки на кін поставлено дуже багато. Пропонований двоетапний підхід дозволяє не втрачати позиції, застосовуючи мобільні рішення, а скористатися їх перевагами. Захищений підхід до мобільної технології – запорука підвищення продуктивності і скорочення операційних витрат держустанов, що в кінцевому підсумку приносить користь усім громадянам, яких вони обслуговують.

Литература:

1. Башинська І.О. Розділ 4.2. Сучасні засоби забезпечення інформаційної складової економічної безпеки промислового підприємства (С. 310-315) у кол. монографії Формування механізму стійкого розвитку економіки: теорія та практика: – Дніпропетровськ: «ФОП Дробязко С.І.», 2014. – 438 с.
2. Bashynska I. Ensuring economic security of modern enterprise as a systematic approach // British Journal of Science, Education and Culture, 2014, No.1. (5) (January-June). Volume IV. “London University Press”. London, 2014. – 804 p. – P. 340-343
3. 2013 Internet Security Report. Електронний ресурс. Режим доступу: http://www.checkpoint.com/campaigns/security-report/download.html
4. The 2014 Mobilometer Tracker: Mobility, Security, and the Pressure In Between. Електронний ресурс. Режим доступу: http://www.mobileworkexchange.com/
5. Bashynskaya I. Organization of the ensuring the informational and analytical safety at the enterprise / Institutionelle Grundlagen für die Funktionierung der Ökonomik unter den Bedingungen der Transformation: Sammelwerk der wissenschaftlichen Artikel.Vol. 2 – Verlag SWG imex GmbH, Nürnberg, Deutschland, 2014. – S. 216-218