УДК 004.056

Ю.В. Борсуковський, В.Л. Бурячок, В.Ю. Борсуковська

БАЗОВІ НАПРЯМКИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ДЕРЖАВНОГО ТА ПРИВАТНОГО СЕКТОРІВ

В даній статті проведено аналіз актуальних кіберзагроз і напрямків їх використання. Сформульовано базові вимоги і рекомендації щодо забезпечення інформаційної та кібернетичної безпеки відповідно до діючих глобальних загроз в інформаційному просторі.

Ключові слова: загрози, ризики, політика, кібербезпека

Вступ та постановка задачі

Травень 2017 року став особливо показовим у плані суперечливості державних і комерційних ініціатив в області кібербезпеки. Всього через два місяці після того, як угруповання кіберзлочинців отримали доступ до спеціальних програмних інструментів Агентства національної безпеки США, хакерська атака вибухнула по всьому світу [1].

Стала очевидна неспроможність багатьох підходів в галузі кібербезпеки. Бадьорі рапорти, концептуальні підходи, гасла і заклики, які озвучувалися з різних трибун, не витримали мінімальної перевірки на здоровий глузд і не змогли протистояти реальній загрозі, що виникла в кіберпросторі.

І це тільки видима частина проблеми забезпечення кібербезпеки державного та приватного секторів. Прихована частина проблеми може дуже серйозно торкнутися внутрішніх питань кібербезпеки в цих секторах. Ці питання згодом будуть тільки загострюватися, оскільки швидко розширюється ландшафт кіберзагроз що дає зловмисникам все нові та нові можливості для широкого використання зовнішніх ознак кіберландшафту з метою приховування внутрішніх інсайдерських атак. Дуже важко, наприклад, відрізнити зовнішню атаку трояна-шифрувальника від внутрішніх зловживань, які можуть бути досить ефективно приховані під імітацією дій шифрувальника (наприклад, шифрування фінансових і складських операцій з метою приховування розкрадань).

Мотиваційні тренди кібератак за 2015-2016 рік добре видно на діаграмі (рис.1.), що наводить Paolo Passeri [6], компанія OpenDNS (тепер Cisco).

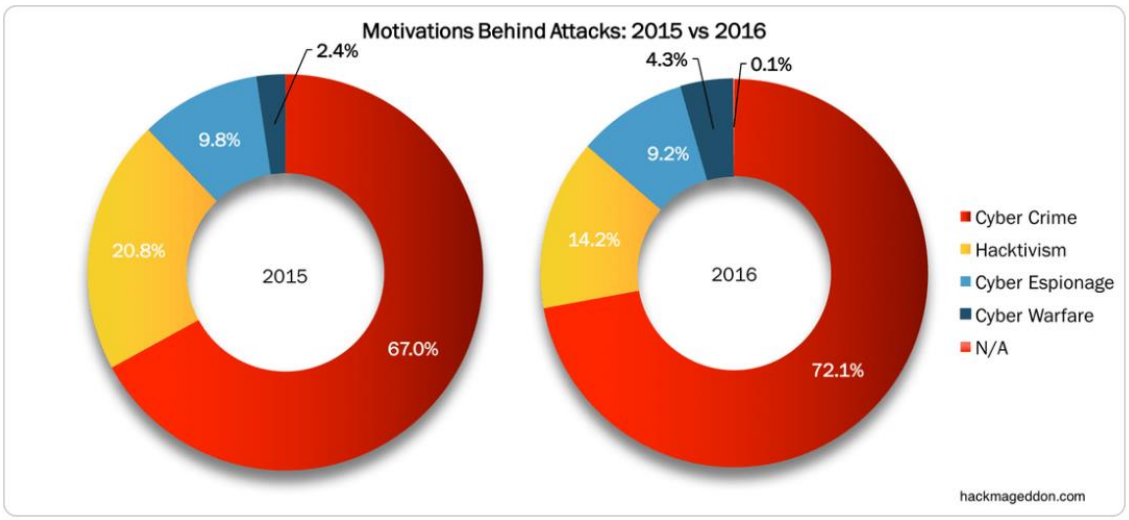

Рис.1. Діаграма кібератак за 2015-2016 роки

Кібербезпека стала предметом, в якому стало дуже важко орієнтуватися. Оцінити рівень загроз і реальність існуючих вимог в області кібербезпеки, спланувати адекватні заходи і вкластися в обмежений бюджет, вибудувати прозорий план стратегічних дій і його поетапну реалізацію з вектором зовнішніх і внутрішніх загроз, що постійно змінюється, стало складно навіть світовим компаніям з сотнями і тисячами фахівців з кібербезпеки.

Тренди цілеспрямованих кібератак будуть тільки рости і цьому буде додатково сприяти широке використання біткоінів в кіберпросторі. Наявність в кіберпросторі віртуальної грошової одиниці значно спрощує «відмивання» грошей для кіберкримінал у. Тепер перетік грошових коштів кіберзлочинцями може здійснюватися без використання додаткових високовитратних сервісів, які коштували десятки відсотків від викрадених сум. Кіберкримінал тепер для розрахунків може використовувати як біткоіни, так і послуги різних платіжних карткових систем. Спрощення перетоків віртуальних біткоінів в матеріальний простір стає додатковим стимулюючим фактором для зростання злочинності в кіберпросторі.

Окремою проблемою в кіберпросторі стане реалізація кіберстратегій на рівні державних політик. Перші і досить насторожуючі результати в геополітичному плані були продемонстровані на виборах президентів в США і Франції, при проведенні референдуму про асоціацію Україна-ЄС в Нідерландах, при інформаційному забезпеченні перекроювання кордонів в Україні, в ході кібератак на енергосистеми України і Прибалтики і т.д.

Публікації WikiLeaks документів і файлів з закритої мережі Центру радіотехнічної і електронної розвідки ЦРУ в Ленглі – по суті елементів кіберзброї, а потім, через дуже короткий термін, їх ефективне використання в кримінальних цілях демонструє дуже ефемерну межу між роботою уповноважених спецслужб в інтересах держави і криміналом [2].

Всі ці фактори дозволяють прогнозувати в найближчій перспективі значне зростання кількості успішно реалізованих зовнішніх і внутрішніх загроз, а, отже, збільшення катастрофічних масштабів наслідків від їх успішної реалізації. Як приклад, атака шифрувальника WannaCry в кіберпросторі викликала хаос в 150 країнах. Найбільш постраждали від його дії Великобританія, Іспанія, Німеччина, Туреччина, Росія, В'єтнам, Японія та ін. Атаковано, за даними Europol, більше 200 000 (по оцінкам фахівців більше 400 000) комп'ютерів. Серед жертв атак виявилися американський гігант FedEx, гігант телекомунікаційних компаній Telefonica і німецька залізнична мережа Deutsche Bahn. Французький автовиробник Renault закрив свій завод в Дуе – один з його найбільших об'єктів, в якому зайнято 5500 осіб [3, 4].

Очевидно, що для світової економіки кіберзлочинність починає представляти серйозну небезпеку, і боротьба з нею повинна отримати пріоритетний характер. Про це було офіційно заявлено в суботу, 13 травня 2007, на зустрічі міністрів фінансів країн G7 в італійському місті Барі. Глава фінансового відомства Італії П'єр Карло Падоан, після закінчення зустрічі, заявив що на ній досягнуто "домовленості з багатьох питань, в тому числі про те, щоб вести боротьбу з кіберзлочинністю, що, на жаль, вельми актуально зараз" [5].

Виклад основного матеріалу

Як видно з вищевикладеного в кіберпросторі починає простежуватися чітка тенденція на використання різних методів для досягнення поставлених цілей. Один і той-же інструментарій може використовуватися як в інтересах уповноважених державних структур так і в інтересах криміналітету.

Виникає необхідність у формулюванні базового переліку питань, заснованих на кращих практиках, який має бути розглянутий і реалізований в комерційних і державних структурах з метою запобігання атак і зменшення ризиків незалежно від існуючого ландшафту кіберзагроз.

Твердження 1. Аналіз ризиків

1. Повинен проводитися регулярний аналіз ризиків у сфері кібербезпеки. Періодичність проведення процедури аналізу ризиків не повинна перевищувати один рік.

2. При виникненні глобальних інцидентів повинен проводитися позаплановий аналіз ризиків з урахуванням зміненого ландшафту кіберзагроз.

Твердження 2. Сканування загроз і патчінг

1. Повинно бути забезпечено регулярне сканування мережі, операційних систем і додатків на наявність вразливостей. Періодичність сканування не повинна перевищувати один місяць.

2. Додатково повинна бути забезпечена регулярна перевірка оновлень додатків третіх виробників і їх встановлення.

3. Повинен існувати план усунення виявлених вразливостей системними адміністраторами.

4. Повинен бути забезпечений щотижневий контроль з боку служби кібербезпеки за процесом усунення виявлених вразливостей системними адміністраторами.

5. Для вразливостей, для яких не існує стандартних засобів їх усунення (патчі), повинні бути передбачені альтернативні способи їх нейтралізації або мінімізації можливих збитків від їх використання.

Твердження 3. Використання білого списку додатків

1. У мережі повинен бути дозволений тільки запуск операційних систем, програм і додатків авторизованих службою кібербезпеки бізнес-структури.

2. Список авторизованих програм і додатків повинен формуватися для кожного профілю користувачів індивідуально.

3. Щорічно список авторизованих програм і додатків повинен підтверджуватися службою кібербезпеки бізнес-структури.

Твердження 4. Забезпечення резервного копіювання

1. Повинно бути забезпечено резервне копіювання всієї критичної інформації.

2. Повинно бути забезпечено створення офлайн-сховища резервних копій. Схема ротації офлайн-сховища повинна гарантувати в кожен момент часу знаходження в 72 годинному офлайні як мінімум однієї резервної копії (термін знаходження офлайн-сховища в недоступному режимі визначається характером критичної інформації та часовою оцінкою можливих загроз).

3. Повинно бути забезпечена регулярна перевірка можливості переходу на резервні копії в разі виникнення будь-яких інцидентів.

Твердження 5. Навчання персоналу

1. Повинно регулярно проводитися навчання персоналу по застосуванню кращих практик в сфері кібербезпеки.

2. Не рідше ніж один раз на рік доцільно «в реальних умовах» проведення навчання персоналу з протидії різним атакам з обов'язковим аналізом створених інцидентів і дій персоналу по їх локалізації (стрес-тестування). Результати підсумкового аналізу з висновками і рекомендаціями повинні доводитися до персоналу.

3. Фахівці з кібербезпеки повинні проходити обов’язкову перепідготовку в спеціалізованих центрах з кібербезпеки не рідше одного разу на три роки.

Твердження 6. Реагування на інциденти

1. Повинен бути розроблений план реагування на інциденти.

2. Служба кібербезпеки повинна регулярно моніторити кіберпростір з метою підтримки план реагування на інциденти в актуальному стані шляхом «проектування» кіберінцидентів на існуючу інфраструктуру бізнесу.

3. План реагування на інциденти повинен тестуватися не рідше ніж один раз на рік.

Твердження 7. Бізнес-безперервність

1. Повинно бути забезпечено чітке розуміння можливостей забезпечення роботи бізнесу без доступу до певних систем.

2. Повинні бути проведені часові та ресурсні оцінки ведення бізнесу без доступу до певних систем.

3. За результатами оцінок повинен бути розроблений план відновлення нормального функціонування бізнесу. Для «вузьких» місць повинен бути складений і затверджений окремий план невідкладних дій.

4. Має проводитися регулярне тестування плану реагування на загрози кібербезпеки і забезпечення бізнес-безперервності.

Твердження 8. Тестування на проникнення

1. Повинні моделюватися й проводитись регулярні спроби атак на власні системи з метою їх дискредитації і перевірки власних можливостей захисту від таких атак.

2. Тестування на проникнення повинно поєднуватися з навчанням персоналу по способам нейтралізації таких атак.

3. За результатами тестування повинні бути внесені зміни і доповнення з усіх питань, які регламентують поточні вимоги з кібербезпеки.

На основі сформульованих тверджень можна визначити базову стратегію служби кібербезпеки по мінімізації ризиків для державних та приватних секторів.

Стратегія 1. Оновлення додатків і операційних систем

Метою більшості атак є вразливі додатки і операційні системи. Застосування останніх оновлень значно зменшує кількість можливих точок входу для хакера. Використовуйте кращі практики, коли оновлюєте ПО, останні оновлення завантажуйте тільки з авторизованих сайтів розробників або постачальників.

Стратегія 2. Білий список додатків

Застосування білого списку додатків це одна з найкращих стратегій кібербезпеки, оскільки дозволяє використовувати тільки спеціально визначені програми і блокує всі інші, включаючи шкідливе програмне забезпечення.

Стратегія 3. Обмеження прав адміністраторів

Кіберзлочинці завжди націлюються на отримання контролю над законними реєстраційними даними, особливо тими, які надають доступ до особливо цінної (конфіденційної) інформації. Обмежте права доступу до рівня, необхідного виключно для цього користувача. відокремте адміністраторів і визначте їх права на окремому рівні, також обмеживши доступ до інших рівнів.

Стратегія 4. Шифрування конфіденційної інформації

Підключіть систему шифрування конфіденційної інформації, що значно обмежить доступ до конфіденційної інформації користувачів з привілейованими правами, а також дозволить зменшити завдану шкоду від її втрати у разі успішної атаки.

Стратегія 5. Сегментація мережі і поділ по зонах безпеки

Сегментуйте мережу по логічним групам і обмежте зв'язки між ПК і головною машиною. Це допоможе захистити конфіденційну інформацію і критичні служби, а також зменшити шкоду від порушення периметра мережі.

Стратегія 6. Перевірка даних, що вводяться

Перевірка даних, що вводяться це метод виключення ненадійних користувачів, що входять нібито як користувачі веб додатків. Цей метод допомагає запобігти багатьом типам зломів безпеки веб додатків, таких як SQL, XSS або командні ін’єкції.

Стратегія 7. Репутація файлів

Підключіть в антивірусному захисті підсистему з перевірки репутації фалів і встановіть максимально жорсткі налаштуваннями. Репутаційні підсистеми можуть обмежувати роботу додатків і дозволяти виконання тільки файлів, які заслуговують надзвичайної довіри, а також зупиняти виконання будь-яких інших недостовірних кодів, не даючи їм можливості отримати контроль над системою.

Стратегія 8. Розуміння технології фаєрволів

Коли хтось або щось може проникнути в вашу систему і в будь-який час, то ймовірно ваша система і стане предметом атаки. Фаєрволи повинні бути налаштовані таким чином, щоб блокувати дані або програми, що надходять з певних локацій (білий список IP адрес), але в той же час, пропускаючи через себе необхідні дані.

Висновки

Використання кращих практик є важливим моментом в захисті мереж, операційних систем і додатків. Виконання цих рекомендацій дозволяє запобігти приблизно 80-85%

цільовим кібератакам на бізнес. Однак не будемо забувати, що при всіх наших зусиллях існує один критичний елемент, який відносять до людського фактору. І тут важливим стає організація процесу безперервного тренінгу персоналу. Багато питань тренінгу можна природним шляхом забезпечити і інтегрувати в сам бізнес. Однак здійснення навчання персоналу методами стрес-тестування і забезпечення безперервності бізнесу може в багатьох випадках виявитися досить проблематичним для практичної реалізації. І тут в процес навчання персоналу можуть бути досить ефективно включені вузи, які займаються підготовкою фахівців з кібербезпеки. Паралельно, при такому системному підході, автоматично вирішується питання з планової перепідготовкою фахівців державного та комерційного секторів з практичних питань кібербезпеки.

Очевидно, що системна побудова зв'язки «бізнес – навчання/перепідготовка - кібербезпека» дозволить вирішувати відразу кілька нагальних завдань, які тісно пов'язані між собою:

1. Бізнес отримує висококваліфіковані кадри в галузі кібербезпеки.
2. Вузи отримують можливість створювати і використовувати сучасну навчальну базу для підготовки і перепідготовки фахівців з кібербезпеки.
3. Кібербезпека переходить в практичну площину, орієнтовану на освоєння кращих практик і безперервну підготовку/перепідготовку персоналу в умовах, наближених до реального ландшафту кіберзагроз.

Все впирається в необхідність вибудовування цілісної системи управління запобіганням кіберзагрозам, підготовки і перепідготовки фахівців та ув'язки її з інтересами і розумінням цього процесу з боку бізнесу. Вибудовування цілісної системи управління запобіганням кіберзагрозам, підготовки і перепідготовки фахівців має проводитися на сучасній матеріальній базі та з залученням високо кваліфікованого викладацького складу.

Системного підходу і повної координації в цьому питанні, нажаль, поки що не видно. Тим не менш всі зовнішні ознаки говорять про те, що це питання вже починає переходити в сферу національної безпеки.

Список використаної літератури

1. BBC. Агентство новин. Травень 13, 2017. [Електронний ресурс] - Режим доступу: http://www.bbc.com/news/technology-39901382?ocid=socialflow_twitter
2. WikiLeaks (@wikileaks). Інтернет ресурс. Березень 7, 2017
3. The New York Times. Травень 14, 2017. [Електронний ресурс] - Режим доступу: https://www.nytimes.com/2017/05/14/world/europe/russia-cyberattack-wannacry-ransomware.html?_r=0
4. AFP – Глобальне інформаційне агентство. Травень 16, 2017. . [Електронний ресурс] - Режим доступу: https://www.afp.com/en/news/205/north-korea-link-emerges-global-cyberattacks
5. Укрінформ - Мультимедійна платформа іномовлення України. [Електронний ресурс] - Режим доступу: https://www.ukrinform.ru/rubric-technology/2227514-ministry-finansov-g7-obavili-vojnu-kiberprestupnosti.html
6. HACMAGEDON Information Security Timelines and Statistics. [Електронний ресурс] - Режим доступу: http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/

Надійшла 16.01.2017 р. Рецензент: д.т.н., проф. Чичикало Н.І.