оприлюдненню на офіційному веб-порталі СБУ; опублікуванню у друкованих виданнях; поширенню в електронній формі тощо.

Таким чином, підсумовуючи, можна визначити, що українське законодавство встановлює два правових режими доступу до публічної інформації. Право на отримання інформації може реалізовуватися у двох формах: пасивній і активній. Але, з огляду на специфіку таа мету і завдання діяльності СБУ, ми вважаємо за доцільне розширити перелік правових режимів доступу до публічної інформації в органах СБУ з двох до чотирьох, а саме закритий, обмежений, процесуальний, повний.

1. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12.

2. Великий тлумачний словник сучасної української мови: 170000 слів / уклад. і гол. ред. В. Т. Бусел; Київ; Ірпінь: Перун, 2003. 1427 с.

3. Рекомендація Ради Європи Комітету Міністрів державам-членам № R (2002) 2 про доступ до офіційних документів, схвалена 02.02.2002 // Доступ до інформації та електронне урядування / авт.-упоряд. М.С. Демкова, М.В. Фігель. Київ: Факт, 2004. 336 с.

4. Коломоєць Т.О. Адміністративне судочинство України: підручник. Київ: Істина, 2008. 256 с.

5. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17.

6. Конституція України від 28.06.1998 р. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

Махницький Олександр Васильович
старший викладач кафедри

Гавриш Олег Степанович
викладач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

АНАЛІЗ КІБЕРЗАГРОЗ. НАЙБЛИЖЧІ ПЕРСПЕКТИВИ

На 26-й найбільшій у світі конференції хакерів DefCon працівник компанії Endgame, що займається системами безпеки, показав програму, яку можна було налаштувати так, щоб вона самостійно створювала шкідливе ПЗ.

Вивчивши середу OpenAl Gym – платформу для тренування ШІ (штучний інтелект), програма навчилася ховати вірус від систем захисту. Система вносила зміни в коректний код, «проводила» його повз антивірус, збирала дані і випускала нову шкідливу версію. Виявити вірус не вдалося.

А якщо шкідлива програма, використовуючи ШІ, зможе автономно визначати, як імітувати нормальну поведінку або рух (наприклад, за допомогою локальних облікових даних), зловмисникам не буде потрібно спеціальний сервер, а шкідливе ПО буде в рази важче ідентифікувати.

У дослідженні компанії Darktrace йдеться про перші зразки програм, які здатні аналізувати оточення. Це дозволяє їм розуміти, де вони перебувають, і знаходити відмінності між віртуалізованим і «голим» середовищем (bare metal), а також знаходити вади в операційній системі.

Така програма зможе підібрати відповідний набір дій для кожного середовища. Коли ІБ-фахівці аналізуватимуть вірус, він буде маскуватися і може залишитися непоміченим. А за справу шкідливий код візьметься вже в руках кінцевого користувача і буде, наприклад, красти коди доступу до банківських рахунків або персональні дані.

Крім цього, використовуючи штучний інтелект, хакери зможуть діяти швидше, ніж фахівці з ІБ, що блокують атаку.

Проаналізувавши ситуацію, ШІ зможе скористатися іншою вразливістю або, не чекаючи на людину, почати пошук альтернативних шляхів злому. В результаті ІБ-шники можуть банально не встигати відображати атаки.

У тому, що штучний інтелект може стати хакерською кіберзброєю, впевнені 62% опитаних ІБ-фахівців. Механізми захисту в найближчі роки теж повинні будуватися із застосуванням ШІ – про це варто замислитися вже зараз, адже з кожною новою адаптацією машинне навчання буде все більш гнучким і легко зможе використовувати знайдені лазівки і уразливості на шкоду сумлінним користувачам.

Розумний фішинг і діпфейки.

Штучний інтелект змінить і фішингові атаки. Завдяки йому цільовоий фішинг (spear phishing), спрямований на обман конкретної людини або компанії, стане ще ефективнішим. Наприклад, троян за прикладом Emotet в дуеті зі штучним інтелектом зможе не тільки розсилати електронні листи, а й розуміти їх контекст і «вдаватися» у справжні ланцюжки електронних листувань.

Вони будуть повністю легітимними, і відрізнити такий фішинг від справжніх імейлів буде майже неможливо. У дослідженні CyberArk 56% з опитаних 1300 осіб, що приймають рішення в IT-безпеки, зазначили, що цільові фішинг-атаки – одна з головних загроз безпеки.

Ще більше посилити фішинг зможуть і діпфейки – фальшиві фото і відео, автоматично створювані алгоритмами з використанням осіб реальних людей. Хакери зможуть використовувати їх як «бонус» до розсилок або як самостійну тактику.

Кіберзлочинці можуть також використовувати цю технологію для маніпулювання цінами акцій, наприклад розмістивши підроблене відео генерального директора, який оголошує, що компанія стикається з проблемою фінансування або якоюсь іншим кризою.

Діпфейкі будуть використовуватися для поширення неправдивих новин на виборах або розпалювання геополітичної напруженості. І абсолютно точно – для того, щоб підвищити ефективність фішингових листів за рахунок, наприклад, фальшивих зображень, згенерованих на базі фото з Фейсбуку.

І якщо раніше всі ці хитрощі вимагали б серйозних ресурсів, тепер вони доступні будь-кому, хто має комп'ютер з потужною відеокартою. Стартапи розробляють технології для виявлення глибоких підробок, але неясно, наскільки ефективними будуть їхні зусилля. Єдина реальна лінія захисту – тренінги з підвищення обізнаності в питаннях безпеки, щоб привернути увагу людей до ризику.

Опенсорсні атаки. У 2018 році можна було спостерігати, як зростає кількість компаній, які постраждали від ланцюжків атак через партнерів або постачальників. Про атаки через третіх осіб (third parties) розповіли 59% опитаних. Ще однією, поки що менш відомою (але не менш небезпечною), підмножиною таких атак стає використання вразливостей ПЗ з відкритим вихідним кодом.

Більшість компаній в умовах браку часу та компетенцій використовують уже кимось написаний код з опенсорсними бібліотеками, доступний для перегляду і змін.

В 2019 р. його уразливості будуть використовуватися ще активніше – якщо раніше ламали конкретний бізнес, то тепер будуть зламувати опенсорс. За прогнозами компанії Black Duck Software, що вивчає опенсорс-проекти, кількість таких атак зросте на 20%.

При цьому, як зазначають експерти, збільшується частка програмного забезпечення з відкритим вихідним кодом. За оцінкою експертів, середня кількість використовуваних опенсорсних бібліотек досягає 147, а близько 60% додатків включають в себе вразливий код, так як подібні баги важко відслідковувати безпосередньо в «продакшені», їх постійні оновлення неможливі, а ось відомості про знайдені вразливості активно публікуються і можуть бути використані шахраями.

Показовий приклад: у листопаді минулого року було виявлено, що хакерам стала доступна широко використовувана JS-бібліотека event-stream, завдяки чому вони впровадили в неї шкідливий код. Розробник передав права на редагування зловмисникові, який вкрав приватні ключі користувачів версій 5.0.2-5.1.0.

В результаті експлуатування уразливості під загрозою опинилися електронні гаманці Copay. Компанія спробувала мінімізувати наслідки атаки і випустила оновлену версію, проте, незважаючи на це, було вкрадено понад 100 біткоїнів.

З одного боку, держава і (меншою мірою) бізнес побоюються закладок в зарубіжному ПО, з іншого – уряд вимагає перевести органи влади і компанії з державною участю на вітчизняне ПО (з часткою в 90% і 70% відповідно до 2024 року).

Цей процес призводить до того, що розробка проводиться поспіхом і часто з використанням опенсорсного коду. На тестування програмних продуктів практично не залишається часу – а отже, формується величезне поле для хакерів, які будуть використовувати невиявлені уразливості.

«Ліками» від цього може стати вбудовування в процес розробки автоматичних сканерів, але поки їх використовують лише одиниці найбільш відповідальних розробників.

Злом смарт-контрактів. Експлуатація смарт-контрактів – ще одна проблема безпеки, яка на нас чекає. Вони починають використовуватися повсюдно: починаючи від грошових переказів і закінчуючи захистом інтелектуальної власності.

Кількість смарт-контрактів уже зросла більш ніж у два рази порівняно з 2017 роком. Разом зі зростом збільшується і кількість вразливостей. Знаходять їх і хакери, які використовують «діри», щоб красти великі суми криптовалют, еквівалентні мільйонам доларів.

Однією з найгучніших історій став злом The DAO – цифрової децентралізованої автономної організації, краудфандінгової платформи. Хакер, використовуючи «лазівку» в смарт-контракті, вивів 3,6 мільйона одиниць криптовалюти Ethereum (близько 60 мільйонів доларів).

Гарантувати безпеку смарт-контрактами можна лише проаналізувавши всі варіанти його виконання. Виконуючи розумні контракти на повних за Тьюрингом мовах, потрібною є впевненість, що комп'ютерна програма не містить багів, що майже неможливо. Тому, створюючи смарт-контракти, доведеться обов'язково проводити їх аудит.

Квантові комп'ютери. Безліч даних шифрується на основі криптографії з відкритим ключем (алгоритм шифрування RSA), в основі якої – факторизация – розкладання числа на прості множники.

Майже всі дані, від транзакцій електронної торгівлі до медичних записів і листування в соціальних мережах, зашифровані саме таким чином. І поки що класичному комп'ютеру не під силу їх розшифрувати.

Але ось квантовий комп'ютер в руках зловмисників впорається з таким завданням за лічені хвилини. Алгоритм Пітера Шора (квантовий алгоритм розкладання чисел на прості множники), запущений на такій машині, призведе до того, що будь-яка інформація в світі стане доступна. Комп'ютер зможе зламувати діючі системи шифрування і робити це на льоту, представляючи загрозу для всієї корпоративної інфраструктури і даних.

Цим вже переймаються вчені: наприклад, у своєму недавньому звіті група американських експертів з квантових досліджень з Національної академії наук, інжинірингу та медицини США закликали компанії впроваджувати нові типи алгоритмів шифрування, які зможуть протистояти квантовій атаці.

Над стандартами нової постквантової криптографії вже працюють і галузеві інститути – цілком ймовірно, вони з'являться через недовгий час після квантових комп'ютерів.

Так, цей ризик може здатися менш актуальним і більш далеким. Але коли справа доходить до кібербезпеки, компанії, які зможуть протистояти загрозам завтрашнього дня, будуть на крок попереду своїх конкурентів.