УДК 004.05(075)
Бортник К.Я., Ломінська Г.Ю.
Луцький національний технічний університет

ТЕХНОЛОГІЇ АНАЛІЗУ НАСЛІДКІВ КІБЕРАТАК

Бортник К.Я., Ломінська Г.Ю. Технології аналізу наслідків кібератак. У статті розкриваються особливості та характеристики кібербезпеки і розглядаються способи, якими фахівці з кібербезпеки аналізують наслідки кібератак. Пояснюються різні категорії вразливостей програмного та апаратного забезпечення та систем безпеки.
Ключові слова: кібербезпека, кіберзлочинність, вразливість.

Бортник К.Я., Ломинский Г.Ю. Технологии анализа последствий кибератак. В статье раскрываются особенности и характеристики кибербезопасности и рассматриваются способы, которыми специалисты по кибербезопасности анализируют последствия кибератак. Объясняются различные категории уязвимостей программного и аппаратного обеспечения и систем безопасности.
Ключевые слова: кибербезопасность, киберпреступность, уязвимость.

Bortnyk K.Ya., Lominskaya G.Yu. Technologies for analyzing the effects of cyber attacks. The article reveals the features and characteristics of cybersecurity and examines the ways in which cybersecurity experts analyze the effects of cyber attacks. Explains the various vulnerabilities of software and hardware and security systems.
Key words: cyber security, cybercrime, vulnerability.

Актуальність проблеми. За оцінками експертів правоохоронних органів країн Центральної та Східної Європи з питань боротьби з комп'ютерною злочинністю, прибутки злочинців від злочинів у сфері використання електронно-обчислювальних машин посідають третє місце після доходів наркоторговців і від продажу зброї.

Одним із досягнень сучасної людини, яка невпинно розвивається в галузі ІТ-технологій стало впровадження в процес управління та інші галузі життя суспільства електронно-обчислювальної техніки, без якої зберігання, обробка та використання дуже великої кількості інформації було б неможливим. Під'єднання до електронної інформаційної мережі стало невід'ємною частиною нашого повсякденного життя. Усі види організацій, такі як медичні, фінансові та навчальні заклади, використовують цю мережу для ефективного функціонування. Вони використовують мережу для збору, обробки, зберігання та обміну великою кількістю цифрової інформації. Оскільки велика кількість цифрових даних збирається та спільно використовується, захист цієї інформації стає ще більш важливим для нашої національної безпеки та економічної стабільності.

У розвиток науки, техніки та інших сфер знань це досягнення принесло неоціненну користь. Однак вигоди, котрі можна отримати завдяки використанню такої техніки, стали використовуватись і в злочинних цілях. Так і з'явився новий вид неправомірної діяльності – комп'ютерні злочини, наслідки яких навіть не йдуть у порівняння зі шкодою від інших злочинів. За оцінками експертів правоохоронних органів країн Центральної та Східної Європи з питань боротьби з комп'ютерною злочинністю, прибутки злочинців від злочинів у сфері використання електронно-обчислювальних машин посідають третє місце після доходів наркоторговців і від продажу зброї, а завдані збитки вже зараз оцінюються мільярдами доларів. Тільки в США щорічно економічні збитки від такого роду злочинів становлять близько ста мільярдів доларів. До середини вісімдесятих років минулого століття у Великобританії збитки від комп'ютерних злочинів становить 750 мільйонів фунтів стерлінгів. В даний час вони зросли вдвічі. Тому питання безпеки – це питання номер один.

Кібербезпека - це постійні зусилля спрямовані на захист мережевих систем та всіх даних від несанкціонованого використання або заподіяння шкоди. На особистому рівні вам потрібно захистити вашу ідентичність, ваші дані та ваші електронні пристрої. На корпоративному рівні відповідальність кожного полягає в захисті репутації організації, даних та клієнтів. На державному рівні це національна безпека, а також на карту поставлено безпеку та добробут громадян.

Конфіденційність, цілісність та доступність, відома як тріада CIA, є керівним принципом для безпеки інформації для організації. Конфіденційність - гарантує конфіденційність даних, обмежуючи доступ до них через механізм аутентифікації. Цілісність гарантує точність і достовірність інформації. Доступність гарантує, що інформація доступна для авторизованих користувачів.

Отже, тепер власне про комп'ютерні злочини. Їх умовно можна розділити на два типи: злочини, що вчиняються прямим втручанням у роботу комп'ютера, і злочини, в яких комп'ютер є необхідним технічним засобом для їх вчинення.

Наведемо до прикладу види злочинів, що пов'язані з втручанням у роботу ПК.

1. Несанкціонований доступ до інформації, що зберігається в комп'ютері.

Такий доступ здійснюється, зазвичай, з використанням несправжнього імені користувача, зміною MAC-адреси пристрою, використанням інформації, що залишилася в історії комп'ютера після виконання деяких операцій, модифікацією програмного та інформаційного забезпечення, розкраданням носія інформації, встановленням засобів запису та копіювання, шо підключаються до каналів передачі даних.

Людей, які здійснюють несанкціонований доступ в чужі комп'ютерні та інформаційні мережі називають "електронними корсарами", "комп'ютерними піратами" або ж просто хакерами.

Несанкціонований доступ до файлів законного користувача здійснюється пошуком слабких місць в захисті системи. Одного разу виявивши їх, порушник може дослідити інформацію, що міститься в системі, копіювати її, повертатися до неї багато разів, подібно до того, як покупець розглядає товари на вітрині.

Програмісти іноді допускаються помилок в програмах, які не вдається виявити в процесі налагодження. Автори великих складних програм можуть не помітити деяких елементарних помилок. Уразливі місця іноді виявляються і в електронних ланцюгах. Всі ці недбалості, помилки призводять до появи "проломів".

Зазвичай вони все-таки виявляються при перевірці, редагуванні, налагодженні програми, але абсолютно позбавиться від них неможливо.

2. Введення в програмне забезпечення "логічних бомб", які спрацьовують при виконанні певних умов і лише частково або повністю виводять з ладу комп'ютерну систему.

"Тимчасова бомба" - різновид "логічної бомби", яка спрацьовує у визначений хакером час.

Такий так званий "троянський кінь", тобто вірус, полягає в таємному введенні в чужу програму таких команд, що дозволяють здійснювати нові, не заплановані власником програми, але вигідні хакеру функції і одночасно зберігати колишню працездатність.

За допомогою "троянського коня" злочинці, наприклад, можуть відрахувати на свій рахунок певну суму з чужого рахунку.

Програмні коди серйозних організацій зазвичай надзвичайно складні. Вони складаються з сотень, тисяч, а іноді і мільйонів команд. Тому "троянський кінь" з кількох десятків команд навряд чи може бути виявлений, якщо, звичайно, немає підозр щодо цього. Але і в останньому випадку експертам-програмістам потрібно багато часу, щоб знайти його.

У США набула поширення форма комп'ютерного вандалізму, при якій "троянський кінь" руйнує через якийсь проміжок часу всі програми, що зберігаються в пам'яті ПК. У багатьох комп'ютерах, що надходять в продаж, виявляють "тимчасову бомбу", яка "вибухає" у найнесподіваніший момент, руйнуючи всю бібліотеку даних. Не слід думати, що "логічні бомби" - це екзотика, невластива нашому суспільству.

Розробка та розповсюдження комп'ютерних вірусів.

"Троянським конем" зазвичай називають комп'ютерні віруси. Вони, вивівши на робочий стіл текст типу: "зітри всі дані цієї програми, перейди у наступну і зроби те ж саме", мають можливість переходити через комунікаційні мережі з однієї системи в іншу, поширюючись як вірусне захворювання.

Виявляється вірус не відразу: перший час комп'ютер зберігає його у собі як звичайну інформацію чи програму, оскільки для маскування вірус нерідко використовується в комбінації з "логічною бомбою" або "тимчасовою бомбою". Вірус спостерігає за всією оброблюваною інформацією і може переміщатися, використовуючи пересилання цієї інформації.

Починаючи діяти (перехоплювати управління), вірус дає команду комп'ютеру, щоб той записав заражену версію програми. Після цього він повертає програмі управління. Користувач нічого не помітить, тому що його комп'ютер знаходиться в стані "здорового носія вірусу". Виявити цей вірус можна, тільки володіючи надзвичайно розвиненою інтуїцією програміста, оскільки ніякі порушення в роботі ЕОМ в даний момент не видають себе. А в один прекрасний день комп'ютер виходить з ладу.Завдяки таким махінаціям, хакери мають змогу заробити не законним шляхом. Експертами зібрано досьє листів від шантажистів, які вимагають перерахування великих сум

грошей в одне з відділень американської фірми "ПК Cyborg"; у разі відмови злочинці погрожують вивести комп'ютери з ладу. Для пошуку і виявлення зловмисників створені спеціальні загони англійських детективів. За оцінкою фахівців в "зверненні" знаходиться більше 100 типів вірусів.

Але всі їх можна розділити на два різновиди, виявлення яких різне за складністю – це "вульгарний вірус" і "роздроблений вірус". Програма "вульгарного вірусу" написана єдиним блоком, і при виникненні підозр у зараженні ЕОМ експерти можуть виявити її на початку поширення. Ця операція вимагає вкрай ретельного аналізу всіх складових операційної системи ЕОМ. Програма "роздробленого вірусу" розділена на частини, на перший погляд, не має між собою зв'язку. Ці частини містять інструкції, які вказують комп'ютеру, як зібрати їх воєдино щоб відтворити і, отже, розмножити вірус. Таким чином, він майже весь час знаходиться в "розподіленому" стані, лише на короткий час своєї роботи збирається у єдине ціле. Як правило творці вірусу вказують йому число репродукцій, після досягнення якого він стає агресивним.

Віруси можуть бути впроваджені в операційну систему, прикладну програму або в мережевий драйвер.

Види вірусів залежать від цілей, переслідуваних їх творцем. Ознаки їх можуть бути відносно доброякісними, наприклад, уповільнення у виконанні програм або поява світлої точки на екрані дисплея (т. зв. "Італійський стрибунець"). Ознаки можуть бути еволютивними, і "хвороба" буде загострюватися в міру своєї течії. Так, з незрозумілих причин, програми починають переповнювати магнітні диски, в результаті чого істотно збільшується обсяг програмних файлів. Нарешті, ці прояви можуть бути катастрофічними і призвести до стирання файлів і знищення програмного забезпечення.

Мабуть, у майбутньому будуть з'являтися принципово нові види вірусів. Наприклад, можна собі уявити (поки подібних повідомлень не було) свого роду "троянського коня" вірусного типу в електронних ланцюгах. Справді, поки мова йде тільки про зараження комп'ютерів. А чому б - не мікросхем? Адже вони стають все більш потужними і перетворюються на подобу ЕОМ. І їх необхідно програмувати. Звичайно, ніщо не може безпосередньо "заразити" мікросхему. Але ж можна заразити комп'ютер, який використовується як програматор для тисячі мікросхем.

Способи розповсюдження комп'ютерних вірусів грунтуються на здатності вірусу використовувати будь-який носій даних, що передаються як "засіб пересування". Тобто з початку зараження є небезпека, що ЕОМ може створити велику кількість засобів пересування і в наступні години вся сукупність файлів і програмних засобів буде заражена. Таким чином, дискета або магнітна стрічка, перенесені на інші ЕОМ, здатні заразити їх. І навпаки, коли "здорова" дискета вводиться в заражений комп'ютер, вона може стати носієм вірусу. Зручними для поширення великих епідемій виявляються телекомунікаційні мережі. Досить одного контакту, щоб персональний комп'ютер був заражений або заразив той, з яким контактував. Однак найпоширеніший спосіб зараження - це копіювання програм, що є звичайною практикою у користувачів персональних ЕОМ. Так скопійованими виявляються і заражені програми.

Фахівці застерігають від копіювання крадених програм. Однак, іноді і офіційно представлені програми можуть бути джерелом зараження.

Природно, що проти вірусів були прийняті надзвичайні заходи, що призвели до створення текстових програм-антивірусів. Захисні програми поділяються на три види: фільтруючі (що перешкоджають проникненню вірусу), проти інфекційні (постійно контролюють процеси в системі) і противірусні (налаштовані на виявлення окремих вірусів).

Однак розвиток цих програм поки що не встигає за розвитком комп'ютерної епідемії.

Зауважимо, що побажання обмежити використання неперевіреного програмного забезпечення швидше за все так і залишиться практично нездійсненним. Це пов'язано з тим, що фірмові програми на "стерильних" носіях коштують чимало у валюті. Тому уникнути їх неконтрольованого копіювання майже неможливо.

Заради справедливості слід зазначити, що поширення комп'ютерних вірусів має і деякі позитивні сторони. Зокрема, вони є, мабуть, кращим захистом від викрадачів програмного забезпечення. Найчастіше розробники свідомо заражають свої дискети яких-небудь нешкідливим вірусом, який добре виявляється будь-яким антивірусним тестом. Це служить досить надійною гарантією, що ніхто не ризикне копіювати таку дискету.

Незалежно від того, яким типом зловмисного ПЗ інфікована система, можна виділити найпоширеніші симптоми того, що пристрій заражено:

- Збільшується навантаження на центральний процесор;
- Знижується швидкодія комп'ютера;
- Комп'ютер часто зависає або дає збої;
- Знижується швидкість перегляду веб-сторінок;
- З'являються незрозумілі проблеми з мережними з'єднаннями;
- Модифікуються файли;
- Видаляються файли;
- Наявність невідомих файлів, програм або значків на робочому столі;
- Запущено невідомі процеси;
- Програми самостійно знімаються з виконання або переконфігуровуються;
- Електронна пошта надсилається без відома та згоди користувача.

Попередження комп'ютерних злочинів.

При розробці комп'ютерних систем, вихід з ладу або помилки в роботі яких можуть призвести до тяжких наслідків, питання комп'ютерної безпеки стають першочерговими. Відомо багато заходів, спрямованих на попередження злочину. Виділимо з них технічні, організаційні та правові.

До технічних заходів можна віднести захист від несанкціонованого доступу до системи, резервування особливо важливих комп'ютерних підсистем, організацію обчислювальних мереж з можливістю перерозподілу ресурсів у разі порушення працездатності окремих ланок, прийняття конструкційних заходів захисту від розкрадань.

До організаційних заходів віднесемо охорону обчислювального центру, ретельний підбір персоналу, виключення випадків ведення особливо важливих робіт лише однією людиною, наявність плану відновлення працездатності центру після виходу його з ладу, організацію обслуговування обчислювального центру сторонньою організацією або особами, незацікавленими в приховуванні фактів порушення роботи центру, універсальність засобів захисту від усіх користувачів (включаючи вище керівництво), покладання відповідальності на осіб, які повинні забезпечити безпеку центру, вибір місця розташування центру і т.п.

До правових заходів слід віднести розробку норм, що встановлюють відповідальність за комп'ютерні злочини, захист авторських прав програмістів, вдосконалення кримінального і цивільного законодавства, а також судочинства. До правових заходів належать також питання громадського контролю за розробниками комп'ютерних систем і прийняття міжнародних договорів про їх обмеження, якщо вони впливають або можуть вплинути на військові, економічні та соціальні аспекти життя країн, що укладають угоду.

Кінець ери відповідності нормам і стандартам в кіберпросторі

У найближчі роки, скоріш за все, тенденція відходу від норм і стандартів під час боротьби з атаками в кіберпросторі буде посилюватись на користь більш творчих рішень. Робота спеціалістів з кібербезпеки буде зосереджена на оцінці реальних загроз і визначення пріоритетності своїх дій, що в свою чергу вимагатиме від них глибокого розуміння проблем, творчого підходу та досить високої експлуатаційної гнучкості.

Висновки. Підсумовуючи усе вище сказане, можна зазначити, що основними тенденціями розвитку ситуації в області кібербезпеки буде поява все більш складних методів кібератак на елементи критичної інфраструктури, посилення інформаційної боротьби в кіберпросторі, зростання загроз для соцмереж, втручання у функціонування бізнесу та проведення фінансових операцій. Наслідком цих тенденцій буде збільшення рівня контролю за користувачами мережі Інтернет, посилення регулювання на національному та міжнародному рівнях діяльності в кіберпросторі, активізація дискусії стосовно збільшення фінансування та інновацій в сектор кібербезпеки, а також покращення фахової підготовки спеціалістів з кібербезпеки.

1. Мастяниця Й.І., Соснін О.В., Шиманський Л.Є. Захист інформаційних ресурсів України: проблеми і шляхи їх розв'язання. - К.: Національний інститут стратегічних досліджень, 2000. - 98 с.
2. П. Браіловський М.М., Головень СМ. та інші. - Технічний захист інформації на об'єктах інформаційної діяльності/ За ред. Проф. В.О. Хорошка. -К.: ДУІКТ, 2007. - 178с
3. https://1391723.netacad.com/courses/623568 Академія Cisco України
4. Kochergin AN Information and spheres of its manifestation: monograph. - Golitsyno: GPI of the Federal Security Service of the Russian Federation, 2008. - 272 p.