Проблеми інформаційної безпеки. Загрози при роботі в Інтернеті і їх уникнення

Поняття інформаційної безпеки

У зв’язку зі зростаючою роллю інформаційно-комунікаційних технологій у сучасному суспільстві проблема захисту даних від втрати, викрадення, спотворення або пошкодження потребує посиленої уваги. Вирішення цієї проблеми сприяє забезпеченню інформаційної безпеки як окремої особистості, організації, так і всієї держави.

Інформаційна безпека — це стан захищеності систем передавання, опрацювання та зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність даних.

Під конфіденційністю розуміють забезпечення доступу до даних на основі розподілу прав доступу, захист від несанкціонованого ознайомлення. До деяких даних право доступу мають усі користувачі, до інших — певні групи людей, а є особисті дані, доступ до яких може мати тільки одна людина.

Деструкція — порушення або руйнування нормальної структури чогонебудь.

Доступність означає забезпечення доступу до загальнодоступних даних усім користувачам і захист цих даних від блокування зловмисниками.

Цілісність передбачає захист даних від їх зловмисного або випадкового знищення чи спотворення.

Також під інформаційною безпекою розуміють комплекс заходів, спрямованих на забезпечення захищеності даних від несанкціонованого доступу, використання, оприлюднення, внесення змін чи знищення.

Останнім часом до питань інформаційної безпеки включено питання інформаційного впливу на особистість і суспільство. У лютому 2017 року указом Президента України було затверджено Доктрину інформаційної безпеки України, яка визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері. Життєво важливими інтер есами суспільства та держави визнано такі:

- захист українського суспільства від агресивного впливу деструктивної пропаганди;
- захист українського суспільства від агресивного інформаційного впливу, спрямованого на пропаганду війни, розпалювання національної та релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;
- усебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності в доступі до достовірних та об’єктивних відомостей та ін.

Загрози інформаційній безпеці

З технічної точки зору, залежно від результату шкідливих дій, можна виділити такі види загроз інформаційній безпеці:

- отримання несанкціонованого доступу до секретних або конфіденційних даних;
- порушення або повне припинення роботи комп’ютерної інформаційної системи;
- отримання несанкціонованого доступу до керування роботою комп’ютерної інформаційної системи;
- знищення та спотворення даних.
- Значна частина загроз інформаційній безпеці виникає внаслідок користування ресурсами Інтернету.

Серед них основними загрозами є такі:

- потрапляння в інформаційну систему шкідливого програмного забезпечення:
  - віруси
  - троянські програми
  - мережеві хробаки
  - клавіатурні шпигуни
  - рекламні системи та ін.;
- інтернет-шахрайство, наприклад: **фішинг** — вид шахрайства, метою якого є виманювання персональних даних у клієнтів онлайн-аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів тощо;
- несанкціонований доступ до інформаційних ресурсів та інформаційно-телекомунікаційних систем, наприклад у результаті цілеспрямованої хакерської атаки — дій, що спрямовані на порушення штатного режиму функціонування системи, порушення доступності її сервісів, отримання несанкціонованого доступу до конфіденційних відомостей, порушення цілісності даних тощо;
- потрапляння комп’ютера до **ботнет-мережі** (англ . botnet від robot і network — робот і мережа) через приховане встановлення програмного забезпечення, яке використовується зловмисником для виконання певних, найчастіше протиправних, дій з використанням ресурсів інфікованих комп’ютерів. Такими діями можуть бути розсилання спаму, добір паролів перебором усіх можливих варіантів, отримання персональних даних про користувачів, крадіжка номерів кредитних карток, паролів доступу, атаки з метою відмови в обслуговуванні, так звані **DDoS-атаки** (англ. **D**istributed **D**enial **o**f **S**ervice — розподілена відмова в обслуговуванні), щоб порушити доступ до деякого інтернет-сервісу шляхом перевантаження його обчислювальних ресурсів та ін.;
- «**крадіжка особистості**» (англ. Identity Theft — крадіжка персональних даних) — несанкціоноване заволодіння персональними даними особи, що дає можливість зловмиснику здійснювати діяльність (підписувати документи, отримувати доступ до ресурсів, користуватися послугами, знімати кошти з банківських рахунків тощо) від її імені.

Загрози для мобільних пристроїв

Ви знаєте, що смартфони — це мобільні телефони, доповнені функціями персонального комп’ютера, зі своєю операційною системою та іншим програмним забезпеченням. Тому для смартфонів характерні ті самі загрози, що і для стаціонарних комп’ютерів: віруси, троянські програми, мережеві хробаки, рекламні модулі (Adware) та ін., орієнтовані на різні

типи мобільних пристроїв. Як і стаціонарні комп’ютери, смартфони можуть потрапити до ботнет-мережі.

Найчастіше смартфон постійно увімкнено, має підключення до мережі Інтернет, завжди розташований поруч із власником, містить різноманітні пристрої введення/виведення: мікрофон, відеокамеру, GPS-навігатор та ін. Часто смартфон забезпечує доступ до грошових рахунків в оператора мобільного зв’язку, у системі онлайн-банкінгу або інших. Усе це підсилює небезпеку.

Існують шпигунські програми, які зловмисники використовують для шпигування за користувачем смартфона. Використовуючи їх, можна перехоплювати повідомлення про всі здійснені дзвінки, дізнаватися вміст СМС-листування та дані про відвідані сайти, знімати камерою телефона оточення користувача, визначати його місце розташування, включати мікрофон і записувати всі розмови.

Ще один аспект загроз для користувачів мобільних телефонів полягає в роботі з платними послугами. Підписка з використанням СМС на онлайн-гру, певний сайт, будь-який сервіс, який вимагає регулярну оплату, може призводити до списування з рахунку знач них коштів. Іноді такі СМС можуть надсилатися троянськими програмами.

Однак не всі користувачі дбають про безпеку та встановлюють антивірусне програмне забезпечення на свої смартфони.

Соціальна інженерія

Соціальна інженерія (англ. social engineering) — це наука, що вивчає людську поведінку та фактори, які на неї впливають.

Термін «соціальна інженерія» як акт психологічної маніпуляції також пов'язують із суспільними науками, однак він широко використовується серед спеціалістів з комп'ютерної та інформаційної безпеки.

Основна тактика соціальної інженерії — за допомогою психологічних методів (наприклад, спілкуючись начебто від імені сервісної компанії чи банку) переконати користувача розкрити інформацію особистого характеру (паролі, номери кредитних карток тощо).

Більшість методів соціальної інженерії не вимагають особливих технічних знань з боку зловмисників, а отже використовувати ці методи може будь-хто — від дрібних злодіїв до досвідчених кіберзлочинців.

Існує багато методик, які підпадають під загальний термін соціальної інженерії в галузі кібербезпеки. Серед найвідоміших методик — спам та фішинг.

Спам — це масове розсилання небажаних листів. Найчастіше спам — це лист електронної пошти, який надсилається одразу на велику кількість адрес, але він також може бути доставлений через миттєві повідомлення,

Фішинг — це форма кібератаки, під час якої злочинець намагається завойовувати довіру до жертви для виманювання конфіденційної інформації. Для отримання даних зловмисники також створюють відчуття терміновості або

SMS та соціальні мережі. Власне, спам не є соціальною інженерією, однак в деяких кампаніях використовуються його види, такі як фішинг, цілеспрямований фішинг (spearphishing), вішинг (vishing), смішинг (smishing), а також поширення шкідливих вкладень або посилань.

застосовують тактику залякування. Варто зазначити, що фішингові кампанії можуть бути націлені на велику кількість випадкових користувачів або конкретну особу чи групу.

Інші методи:

Цілеспрямований фішинг — це форма фішингу, під час якої зловмисник надсилає повідомлення,спрямовані на конкретну групу людей, або навіть просто окрему особу з метою викрадення даних або маніпулювання ними в зловмисних цілях.

Вішинг та смішинг — це методи соціальної інженерії, подібні до фішингу, але здійснюються не через електронну пошту. Зокрема, вішинг реалізовується через шахрайські телефонні дзвінки, а для смішингу використовуються текстові SMS-повідомлення, які містять шкідливі посилання або вміст.

Видавання себе за іншу особу є іншим популярним методом соціальної інженерії, під час якого кіберзлочинці діють нібито від імені певної особи, вводячи в оману потенційних жертв. Типовим прикладом є зловмисник, який видає себе за генерального директора певної компанії, укладає та затверджує шахрайські угоди в той час, як справжній генеральний директор перебуває у відпустці.

Афери з технічною підтримкою — це, зазвичай, неправдиві телефонні дзвінки або Інтернет-реклама, в якій зловмисники пропонують жертвам послуги служби технічної підтримки. Насправді, кіберзлочинці просто намагаються заробити гроші, продаючи фейкові послуги або усуваючи насправді неіснуючі проблеми.

Шкідливе програмне забезпечення, ціль якого викликати у жертви почуття страху чи тривоги та таким чином змусити її встановити небезпечний код на пристрій. Поширеними є випадки, коли користувачам відображалось повідомлення про нібито інфікування пристрою загрозою, для видалення якої необхідно завантажити антивірус (який, насправді, є шкідливим програмним забезпеченням).

Кібершахрайство — це схеми зловмисників, у яких часто використовують один або навіть декілька методів соціальної інженерії, описаних у цьому розділі.

Правила безпечної роботи в інтренеті

Основні правила безпечної роботи в Інтернеті:

- Використовуйте тільки ліцензійне програмне забезпечення. Установлюйте програми тільки з офіційних джерел. Перед установленням читайте відгуки інших користувачів, якщо вони доступні.
- Установлюйте та оновлюйте антивірусне програмне забезпечення як на стаціонарні, так і на мобільні комп’ютери. Бажано, щоб оновлення антивірусних баз здійснювалося регулярно та автоматично.
- Завжди встановлюйте оновлення операційної системи та іншого програмного забезпечення.
- Використовуйте надійні паролі. Не використовуйте на різних інтернет-ресурсах один і той самий пароль, змінюйте його регулярно.
- Приєднуйтеся тільки до перевірених Wi-Fi-мереж. Не відправляйте важливі дані (дані кредитних карток, онлайн-банкінгу тощо) через публічні та незахищені Wi-Fi-мережі.
- Установіть фільтр спливаючих вікон у браузері.
- Перевіряйте сертифікат безпеки сайтів у вигляді замка в адресному рядку браузера.
- Не відкривайте повідомлення електронної пошти від невідомих вам осіб і прикріплені до них файли, яких ви не очікуєте.
- Подумайте про можливі ризики для вас перед тим, як викласти щось у мережу Інтернет.
- Створюйте резервні копії важливих для вас даних, зберігайте їх на носіях даних, відключених від мережі Інтернет.

Постійно купуєш товари в Інтернеті?

- Під час здійснення покупок онлайн використовуй тільки перевірені сайти Інтернет-магазинів.
- Для здійснення онлайн-платежів користуйся спеціальним захищеним браузером.
- Завантажуй додатки тільки з офіційних банківських сайтів. Оскільки зловмисники часто поширюють підроблені банківські програми для викрадення особистої інформації.
- Не використовуй підозрілі онлайн-форми для введення банківських даних.

Перебуваєш в мережі 24/7?

- Уникай підключення до публічних мереж Wi-Fi.
- Використовуй домашню мережу або мобільний Інтернет, особливо під час здійснення онлайн-транзакцій або передачі конфіденційних даних.
- Налаштовуй автоматичні оновлення додатків та програмного забезпечення.
- Використовуй антивірусне програмне забезпечення для безпеки девайсів.

Таємно переглядаєш романтичні мелодрами про кохання?

- Для безпечного перегляду відео використовуй тільки захищені веб-сайти. Крім цього, будь обережним під час використання спеціальних розширень браузера, які можуть містити шкідливий код.
- Не натискай на підозрілі рекламні банери та спливаючі рекламні оголошення.
- Встанови надійне антивірусне рішення на всі девайси, а також забезпеч захист смарт-телевізора від несанкціонованого доступу хакерів.
- Контролюй кількість підключених пристроїв до домашнього роутера.

Ти активний користувач соціальних мереж?

- Для захисту персональних даних в соціальних мережах створюй надійні паролі, які не містять шаблонних фраз та окремих слів, замість цього використовуй складні речення, наприклад, назви книг або цитати відомих людей.
- Використовуй двофакторну аутентифікацію для покращення безпеки облікових записів. У разі викрадення паролю аутентифікація допоможе захистити акаунт від несанкціонованого доступу.
- Створюй унікальний пароль до кожного акаунту в мережі Інтернет. Оскільки застосування одного пароля для багатьох профілів підвищує уразливість конфіденційних даних.

Не можеш прожити ні хвилини без смартфона?

- Щоб твій гаджет не опинився під контролем зловмисників, дотримуйся основних правил безпеки для захисту мобільних девайсів. Зокрема, для завантаження програм використовуй тільки офіційні магазини додатків.
- Завантажуй додатки лише перевірених розробників. Крім цього, читай відгуки інших користувачів, особливо звертай увагу на негативні коментарі.
- Здійснюй регулярне оновлення операційної системи та кожного додатку для виправлення уразливостей.

Джерела

- miyklas.com.ua
- Соціальна інженерія
- Соціальна інженерія (безпека))
- www.eset.com
- www.eset.com