БЕЗПЕКА В ІНТЕРНЕТІ

Коваленко К.М., ст. гр. А-31-17
Думанецький Д.І.,ст. гр. А-31-17
Костікова М.В. –керівникканд. техн. наук, доцент
ХНАДУ

Введення. Усе життя людини – це бурхлива буря подій, яка таїть в собі небезпечні моменти, від котрих ми повинні вміти захиститися. Особливо зараз, коли сучасне життя неможливе без інтернету. Ми використовуємо доступ до мережі для пошуку, публікації та обробки інформації. Але чи росте рівень знань про те, як протистояти кіберзагрозам? Особливо враховуючи, що сьогодні в результаті злому аккаунта можна втратити набагато більше, ніж на зорі рунета.

Переваги використання інтернету очевидні. Як будь-яка складна інфраструктура, інтернет містить багато небезпек, нехтування якими може призвести не просто до втрати спокою, але й істотних грошових коштів. Кожен, хто працює з мережею, щоб не випробовувати на собі її «темні» сторони, повинен знати потенційні джерела небезпеки та вміти захищати себе й своїх менш «просунутих» близьких і друзів від шахраїв. Вони завдяки шахрайським маневрам можуть заволодіти вашими особистими даними.

Є багато джерел небезпеки в Інтернеті це: комп'ютерні віруси і троянські програми; мережеві атаки; соціальна інженерія; фішингові сайти та розсилки; соціальний ексгібіціонізм.

Комп'ютерні віруси и троянські програми. Комп'ютерний вірус – це програмне забезпечення з можливостями самокопіювання, впровадження в системний код та інші програмні продукти, а також нанесення непоправної шкоди апаратної частини комп'ютера і інформації, що зберігається на його носіях.

Шкідливе програмне забезпечення отримало назву «вірус» за свою схожість з біологічним прототипом. Він так само може мати стадію інкубації, і так само самостійно розмножується і паразитує в операційній системі комп'ютера. Таким чином, комп'ютерним вірусом є ПО з небезпечними для систем машини властивостями.

Троянська програма – це особливий різновид програмної закладки. Вона додатково наділена функціями, про існування яких

користувач навіть не підозрює. Коли троянська програма виконує ці функції, комп'ютерній системі наноситься певний збиток. Однак те, що за одних обставин заподіює непоправної шкоди, при інших - може виявитися цілком корисним. Приміром, програму, яка форматує жорсткий диск, не можна назвати троянської, якщо вона якраз, і призначена для його форматування (як це робить команда format [parameter] операційної системи DOS або Windows). Але якщо користувач, виконуючи деяку програму, абсолютно не чекає, що вона отформатує його вінчестер, – це і є справжнісінький троянець.

Трояни і віруси можуть бути приховані в безкоштовних, доступних для скачування з інтернету програмах або на піратських дисках.

Як це працює: ви запускаєте програму, і вона, використовуючи відому зловмисникові вразливість вашої операційної системи або іншої програми, захоплює контроль над комп'ютером. З цього моменту вірус чи троян безперешкодно володіє комп'ютером, доставляючи масу неприємностей виконуючи неочікувані для вас дії. Трояни при цьому щедре діляться вашою персональною та фінансовою інформацією зі своїм господарем, відправляючи її по інтернету.

Мережеві атаки. Мережеві атаки – це спроба знайти вразливі місця в його операційній системі й програмах, які можуть бути використані зловмисником для різних цілей, наприклад: виведення вашого комп'ютера з ладу; відключення його від інтернету (у випадку, якщо комп'ютер є сервером, що надає якийсь корисний інтернет-сервіс клієнта, це може спричинити за собою репутаційні й фінансові втрати, якщо він не зможе надавати ці послуги); запуск на вашому комп'ютері шкідливої програми; крадіжка ваших даних; блокування ваших даних з метою шантажу; додавання вашого комп'ютера під шкідливий бот-нет.

І це далеко не повний перелік цілей зловмисників.

Існує величезна безліч різних конфігурацій комп`ютерів, операційних систем і мережевого устаткування, однак, це не стає перешкодою для доступу в глобальну мережу. Така ситуація стала можливою, завдяки універсальному мережевого протоколу TCP / IP, який встановлює певні стандарти і правила для передачі даних через інтернет. На жаль, подібна універсальність призвела до того, що комп`ютери, що використовують даний протокол, стали уразливі для зовнішнього

впливу, а оскільки протокол TCP / IP використовується на всіх комп`ютерах, підключених до інтернету, у зловмисників немає необхідності розробляти індивідуальні засоби доступу до чужих машин.

Як це працює: з комп'ютера зловмисника, чи зараженого спеціальним вірусом комп'ютера ще однієї жертви через інтернет або іншу мережу, проводиться спроба підключення до комп'ютера жертви за допомогою знайденої вразливості. Метою мережевої атаки може бути й сам пошук такої вразливості.

З початком широкого використання міжнародних мереж передачі даних загального користування темпи росту мережної злочинності зростають в геометричній прогресії. За оцінками експертів Міжнародного центру безпеки Інтернет (CERT) кількість інцидентів пов'язаних з порушенням мережної безпеки зросла в порівнянні з 2000 роком майже у 10 разів.

Основними причинами, що провокують ріст мережної злочинності є недосконалі методи і засоби мережного захисту, а також різні уразливості у програмному забезпеченню елементів, що складають мережну інфраструктуру.Основними джерелами небезпек для користувачів Інтернету являється діяльність хакерів, вірусів та спамів. Існують засоби, що утруднюють доступ до чужих комп'ютерів – це брандмауери, антивірусне та антиспамове програмне забезпечення. Велике значення також має дотримання користувачами правил безпеки під час роботи в Інтернеті.

Для отримання персональної інформації, небезпечні особи використовують чати, системи обліку миттєвими повідомленнями та сайти знайомств. Дотримання простих правил в спілкуванні через мережу Інтернет, дозволить захистити користувача від недобрих намірів зловмисників.

Насправді, що таке Інтернет? Електронний океан, таємнича стихія, ув'язнена в кремнієвих кристалах і мідних проводах сучасних комп'ютерів. Неіснуючий всесвіт, що інший раз здається реальнішою, ніж наш матеріальний, «справжній» світ. Те, що вторгається в кожен будинок, обвиває всю планету і свідомість всіх людей тугою мідно-кремнієвою павутиною; щось позамежне, незбагненне людському розуму, нікому не видиме, але всіма що відчувається.