Курс "Сучасні технології безпечного програмування"

Давидов Вячеслав Вадимович

Мета та задачі курсу

- **Мета курсу**: розглянути основні помилки при програмуванні, а також проектуванні, які призводять до найбільш поширених, небезпечних та руйнівних вразливостей програмного забезпечення.
- **Задачі курсу:**
  - Виявляти найпоширеніші програмні помилки, які призводять до вразливості програмного забезпечення, розуміти, як ці помилки використовуються зловмисниками та як реалізовувати свої рішення безпечним чином.
  - Виявляти ризики та наслідки вразливості програмного забезпечення для виявлення основних напрямків діяльності щодо розробки безпечного програмного забезпечення.
  - Освоїти прийомам програмування, які допоможуть уникнути розвитку шкідливих звичок та дозволять розробляти безпечні програми під час вашої професійної кар’єри.

Кіберзлочинність

- Кіберзлочинність - злочинна діяльність, що здійснюється з використанням комп'ютерів та/або через мережі чи Інтернет. Може призвести до втрати авторитету, а також частини ринку. Щорічні втрати від кіберзлочинності сягають мільярдів доларів на рік.
- Типи кіберзлочинності:
  - **Фішинг** —отримання доступу до конфіденційних даних користувачів — логінів та паролів.
  - підроблені антивіруси
  - порушення авторських прав - "піратство". **Стаття 177 УК України**.
  - шахрайство з платіжними картками, АТМ
  - **тайпсквоккінг** - реєстрація доменних імен, близьких за написанням з адресами популярних сайтів з розрахунку на помилку частини користувачів: https://vkontrakte.ru/
  - **Сніффінг** – відстеження трафіку для отримання конфіденційної інформації
  - **Соціальна інженерія** - метод отримання необхідного доступу до інформації, що ґрунтується на особливостях психології людей
  - **Кібер-сквоккінг** - реєстрація доменних імен, що містять торгову марку, що належить іншій особі з метою їх подальшого перепродажу або недобросовісного використання

Кіберзлочинність. Фішинг

- **Фішинг** - Один із різновидів соціальної інженерії, заснований на незнанні користувачами основ мережевої безпеки: зокрема, багато хто не знає простого факту: сервіси не розсилають листів з проханнями повідомити свої облікові дані, пароль та інше.
- **Техніка фишингу:**
  - Соціальна інженерія
  - Веб-посилання
    - https://www.privatbank.mybank.com/
    - http://good
    - http://www.google.com@members.tripod.com/
    - Інтернаціональні домени

Кіберзлочинці

- Хакери. Хакери хакерам різниця:
  - White Hats – працює легально (кіберполіція), забезпечує захист даних, виявляє вразливості та допомагає позбутися їх.
  - Grey Hats – здійснюють нелегальний злом без злого наміру та мети отримати прибуток (дослідники, творці своєї системи безпеки на основі недокументованих «проблем» у «конкурентів»).
  - Black hats – завдають шкоди. Незаконний злам пристроїв, систем, мереж з метою отримання прибутку
- Інсайдери
- Професійна/конкуруюча розвідка
- Кібертерористи

Комп'ютерна безпека

- Безпечна розробка - реалізація бездоганних та безпечних конструкцій коду (відповідає розробник)
- Операційна безпека - захист систем та мереж від атак (відповідає системний адміністратор)

Інформаційна безпека

- Доступність (**A**vailability)
- Цілісність (**I**ntegrity)
- Конфіденційність (**C**onfidentiality)
- Невідмовність (non-repudiation)
- Підзвітність (належність) (accountability)
- Автентичність (authenticity)
- Достовірність (reliability)

Забезпечення інформаційної безпеки

- Оцінка вартості
- Розробка політики безпеки
- Реалізація політики безпеки
- Кваліфікована підготовка спеціалістів
- Аудит

Дефекти ПЗ

- Помилка бізнес логіки
- Недоліки безпеки (security flaw) – дефект ПЗ, що створює потенційну загрозу безпеці

Вразливості

- Вразливість - набір умов, що дозволяють зловмиснику порушити явну чи неявну безпекову стратегію. Уразливості у програмному забезпеченні є суб'єктом діяльності зловмисників. Використання вразливостей може набувати безліч форм, включаючи черв'яки, віруси та троянські коні.
- Не всі дефекти – недоліки безпеки ведуть до вразливості. Такі дефекти можуть зробити програму вразливою для атаки, коли вхідні дані програми (наприклад, параметри командного рядка) перетинають межу безпеки, визначену операційною безпекою.
- Вразливості можуть бути без недоліків безпеки. Оскільки безпека є атрибутом якості, для якого слід шукати компроміс з іншими атрибутами, такими як продуктивність та зручність використання, розробники програмного забезпечення можуть навмисно залишити свій продукт вразливим для того чи іншого злому. Навмисне рішення не усувати вразливість не означає, що програмне забезпечення є безпечним, воно означає лише те, що розробник погоджується із цим ризиком від імені споживача ПЗ
- Експлойт – технологія використання вразливості безпеки для явного чи неявного порушення стратегії безпеки.

Контрзаходи

- Контрзаходи - рішення для усунення нестачі програмного забезпечення або обхідний шлях, який може застосовуватися для запобігання/обмеження використання вразливості
  - На рівні вихідного коду контрзаходи можуть виявитися дуже простими, наприклад, проста заміна операції копіювання необмеженого рядка копіюванням з обмеженнями.
  - у деяких випадках більш економічно ефективним може бути усунення нестачі безпеки шляхом запобігання його досягненню зловмисником (ізоляція вразливості або запобігання доступу шкідливих вхідних даних до вразливого коду, наприклад, за допомогою операційної безпеки).
  - На рівні системи або мережі контрзаходи можуть включати відключення порту або фільтрацію трафіку, щоб запобігти зловмиснику доступу до вразливості