УДК 004.491
Г.В. Рожко
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ОСНОВНІ ВИДИ ЗАГРОЗ ІНФОРМАЦІЇ

G.V. Rozko

MAIN TYPES OF THREATS TO INFORMATION

Одне із первинних завдань для нормального функціонування комп'ютерної мережевої системи (КМС) і можливості успішного ведення бізнесу є безпека інформаційних потоків, які в ній циркулюють.

У загальному випадку існують наступні базові види загроз [1]: порушення конфіденційності; порушення цілісності; порушення доступності; порушення спостережності; порушення автентичності.

Кожній приведеній вище загрозі відповідає відповідна надана послуга захищеної системи, тобто, послуга конфіденційності, цілісності, доступності, спостережності і автентичності відповідно. Система при цьому вважається захищеною або безпечною, якщо забезпечує усі вищезгадані послуги [2].

Усі погрози для корпоративних мереж в загальному випадку можуть бути поділені на дві категорії [2]: погрози, які виходять від зловмисника; погрози, пов'язані з реалізацією, підтримкою або з порушенням середовища функціонування.

Погрози, які виходять від зловмисника [2]: перехоплення конфіденційної інформації - порушення конфіденційності; не санкціоновані джерелом модифікації або створення інформації від його імені - порушення цілісності; помилкова відмова джерелом факту формування і передачі інформації певному одержувачеві в заданий час - порушення автентичності; помилкове затвердження одержувачем факту отримання інформації від певного джерела в заданий час - порушення автентичності; помилкове затвердження джерелом факту формування і передачі інформації певному одержувачеві в заданий час - порушення автентичності; помилкова відмова одержувачем факту отримання інформації від певного джерела в заданий час - порушення автентичності; несанкціонована зміна алгоритмів функціонування деякої підсистеми КІС - можлива будь-яка базова загроза; блокування працездатності деякої підсистеми (web, pop, smtp сервери) - порушення доступності.

Погрози, пов'язані з реалізацією, підтримкою або з порушенням внутрішнього середовища функціонування: невірна з точки зору безпеки реалізація і розгортання продукту; невірна підтримка і адміністрування продукту; порушення середовища функціонування продукту.

Насправді, правильна реалізація продукту має на увазі, надійну аутентифікацію і авторизацію користувача, а також захищені канали зв'язку з ним і між складовими частинами системи. Ці чинники безпосередньо зменшують приведені погрози, пов'язані з порушником. Крім того, вірна реалізація продукту має на увазі певне налаштування його складників і використовуваних технологій, що зменшує ризик неправильної підтримки і адміністрування продукту.

Література

1. Столлингс В. Криптография и защита сетей: принципы и практика / В. Столлингс; пер. с англ. А. Жемякина; [ред. И. Тригуб]. – 2-е издание. – М.: Издательский дом "Вильямс", 2001. - 672 с. – ISBN: 5-8459-0185-5.

2. Конеев И.Р. Информационная безопасность предприятия / И.Р. Конеев, А.В. Беляев. – СПб.: BHV-Петербург, 2003. – 752 с. – ISBN: 5-94157-280-8.