Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій

(повна назва)

Кафедра Інфокомунікаційної інженерії імені В.В. Поповського

(повна назва)

**АТЕСТАЦІЙНА РОБОТА**

**Пояснювальна записка**

перший (бакалаврський)

(освітньо-кваліфікаційний рівень)

Тестування на проникнення корпоративної мережі компанії

(тема роботи)

Виконав: студент 4 курсу, групи КУІБу-18-1

Спеціальність: 125 Кібербезпека

(шифр і назва спеціальності)

Данилюк А.О

(прізвище, ініціали)

Керівник Агеєв Д.В

(прізвище, ініціали)

Допускається до захисту

Зав. кафедри \_\_\_\_\_\_\_\_\_\_\_ Лемешко О.В

(підпис) (прізвище, ініціали)

2021 р

1 АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ

* 1. Корпоративні мережі, як основа ведення бізнесу

Одним з найбільших переваг, які надихають власників бізнесу на побудову корпоративних мереж, є їх можливість підвищити прибуток від бізнесу.

Оскільки за допомогою мереж організовується один інформаційний простір в рамках підприємства, всі учасники робочого процесу отримують до інформації вільний доступ в режимі реального часу. Це дозволяє значно скоротити витрати на кур'єрів і пересилку кореспонденції. Крім того, підвищується оперативність реакції на всі зміни в інформаційному полі, що веде до зниження втрати часу. Для керівників бізнесу мережі також дуже корисні, оскільки вони дають можливість контролювати всі робочі процеси і виконання будь-яких операцій. Підвищення прибутку - це дуже позитивний фактор, але для прогресивних керівників важливо, щоб корпоративні мережі в офісі допомагали не тільки заощадити, але і стрімко розвиватися. Головна цінність корпоративних мереж полягає в тому, що необхідну інформацію можна отримати в лічені хвилини. Як відомо, той, хто володіє інформацією, той і на коні. Отже, за допомогою високої швидкості обробки даних і оперативного доступу до них можна будувати ефективні стратегії розвитку компанії. Крім того, для проведення ділових переговорів і організації конференцій необов'язково їздити в інші міста або країни, все це можна організувати за допомогою конференц-зв'язку і відеозв'язку. Отже, розширюється поле для пошуку ділових партнерів та комунікації з ними.

Офісна корпоративна мережа має такі переваги:

* дає змогу зв’язати всю техніку в одну мережу;
* дає моментальний доступ до всієї корпоративної інформації в режимі реального часу;
* дозволяє швидко обробляти дані;
* надає засоби і інструменти для передачі інформації;
* робить ведення бізнесу більш прозорим;
* дозволяє оперативно реагувати на всі зміни;
* створює чудові умови для розвитку бізнесу.
  1. Розповсюджені проблеми безпеки корпоративних мереж

Існує безліч загроз мережевої безпеки, про які слід знати підприємствам, щоб забезпечити безперервний захист своїх систем, програмного забезпечення і даних. Десять основних загроз мережевої безпеки і рішення, які можна використовувати для захисту своєї мережі від злому цими шкідливими атаками.

1. Шкідливі програми / програми-вимагачі. В теперішній час, підприємства стають жертвами атак програм-вимагачів кожні 14 секунд. Ці атаки програм-вимагачів ростуть більш ніж на 350% щорічно, при цьому кількість атак на системи інтернет речей збільшується на 217,5% в річному численні з 2019 по 2020 рік.

Настільки масове зростання числа програм-вимагачів було викликано створенням криптовалют, які дозволяють хакерам анонімно вимагати викуп. Ці витончені атаки починаються з зараження захищених систем баз даних, шифрування даних і загроз видалення або пошкодження файлів, якщо не буде сплачено викуп. Проактивність стратегії відновлення програм-вимагачів і зберігання резервних копій даних в мережі гарантує, що ви не зіткнетеся з втратою даних, перериванням роботи і додатковими витратами, пов'язаними з необхідністю платити викуп.

1. Ботнети. Хоча технічно це не шкідливе ПО, ботнети в даний час вважаються однією з найбільших загроз в Інтернеті. Цими потужними мережами скомпрометованих машин можна дистанційно керувати і використовувати їх для масованих атак. Кожен ботнет запускає безліч комп'ютерів-зомбі, які використовуються для проведення ретельних розподілених атак типу «відмова в обслуговуванні» (DDoS) (ми повернемося до них пізніше). Ці атаки використовуються, щоб знищити жертву, змусити її заплатити викуп щоб повернути собі контроль над своєю системою.
2. Комп’ютерні віруси і черв’яки. Статистика показує, що приблизно 33% домашніх комп'ютерів схильні до яких-небудь шкідливих програм, більше половини з яких - віруси. Віруси прикріплюються до системного або хост-файлу і можуть не діяти до тих пір, поки не будуть випадково активовані таймером або подією. З іншого боку, черви заражають документи, електронні таблиці та інші файли, іноді використовуючи макроси. Як тільки вірус або черв'як потрапляє в вашу систему, він негайно починає реплікувати себе з єдиною метою - заразити якомога більше мережевих систем і недостатньо захищених комп'ютерів. Передача вірусів і черв'яків часто здійснюється за допомогою вразливостей програмного забезпечення. Як тільки вони знайшли свою нішу у вашій системі, вони поширюються як лісова пожежа, зачіпаючи як можна більше компонентів системи і користувачів.
3. Фішингові атаки. Фішингові атаки - це форма соціальної інженерії, яка призначена для крадіжки конфіденційних даних, таких як паролі, імена користувачів, номери кредитних карт. Ці атаки видають себе за веб-сайти з хорошою репутацією, банківські установи та особисті контакти, які приходять в формі миттєвих повідомлень або фішингових листів, які виглядають законними. Після того, як ви натиснете «Відповісти» або клацнете вбудований URL-адресу в цих повідомленнях, вам буде запропоновано використовувати свої облікові дані або ввести свої фінансові дані, які потім відправлять вашу інформацію зловмисному джерелу.
4. DDoS (розподілена відмова в обслуговуванні). Перевантаження розміщених серверів і їх повна непрацездатність - це завдання кібератаки, відомої як атака розподілена відмова в обслуговуванні (DDoS). За статистикою 33% підприємств стають жертвами DDoS-атак. DDoS-атаки можуть мати катастрофічні наслідки для компаній, які заробляють гроші на роботі в Інтернеті (соціальні мережі, сайти електронної комерції і т. Д.), Потенційно викликаючи втрату доходу в мільйони доларів кожен день, коли веб-сайт не працює. Ймовірно, що не всі з потенційно тисяч комп'ютерів, що використовуються для DDoS-атаки, насправді належать зловмисникові. Замість цього можна припустити, що більшість скомпрометованих комп'ютерів додані в мережу зловмисника за допомогою шкідливого ПО і поширюються по всьому світу через ботнет.
5. Криптоджекінг. Ще до того, як біткойн стрімко злетів в 2017 році, кріптоджекінг був улюбленим інструментом хакерів, які прагнуть вкрасти криптовалюта у нічого не підозрюють жертв для отримання фінансової вигоди. Ці атаки схожі на черв'яків і вірусів, за винятком того, що замість пошкодження конфіденційних даних і інформації, кінцевою метою кріптоджекінга є крадіжка ресурсів ЦП. За допомогою експлойтів кріптоджекінга хакери обманом змушують своїх жертв завантажувати коди для майнінгу на свої комп'ютери, а потім використовують ці шахрайські коди для доступу до ресурсів обробки ЦП для майнінгу криптовалют.
6. Розширені постійні погрози (скорочено APT). Це кібератаки, які вимагають, щоб неавторизований зловмисник закодував свій шлях в нічого не підозрюючу системну мережу, залишаючись там непоміченим протягом досить довгого часу. Замість того, щоб розкривати свою позицію, APT перекачує фінансову інформацію та іншу важливу інформацію про безпеку з мережі жертви. Архітектори APT вміють використовувати різні методи для отримання доступу до мережі; використовуючи для цього шкідливі програми, набори експлойтів і інші витончені засоби. Після того, як зловмисник подолав мережевий брандмауер, він не діє, поки не виявить облікові дані для входу, за якими прийшли. Після отримання цих облікових даних APT поглиблюється в мережу, щоб заразити інші частини системи, скомпрометувавши якомога більше форм даних.
7. Троянський кінь або «троян» - це програма, яка виглядає законною, але насправді заражена безліччю вірусів. Як тільки троянський кінь отримує доступ до мережі, його можна використовувати для реєстрації натискань клавіш з метою крадіжки конфіденційної особистої інформації. Атаки троянських коней часто поширюються по електронній пошті аналогічно тому, як фішингова атака використовує мережу. Коли користувачі натискають на електронний лист (яке нібито відправлено кимось, кому можна довіряти), вони знаходять вкладення, яке автоматично завантажує шкідливе ПО на комп'ютер жертви. Як тільки троян отримає доступ до вашого комп'ютера, він може навіть захопити вашу веб-камеру і використовувати ваші конфіденційні дані та інформацію, щоб використовувати вас на кожному вашому кроці.
8. Руткіт. Руткіти - це набір інструментів, які розміщуються в мережі зловмисником, що скористався уразливістю системи безпеки. Зловмисник використовує руткіт для забезпечення віддаленого доступу до системи жертви і отримання доступу на рівні адміністратора в своїй мережі. Після підключення віддаленого доступу руткіти мають намір виконувати зловмисні атаки, включаючи (але не обмежуючись) реєстрацію ключів, крадіжку паролів, відключення антивіруса і багато іншого.
9. Атака з використанням SQL-ін'єкції. Атаки з використанням SQL-ін'єкцій використовують шкідливий код для використання вразливостей системи безпеки і отримання або знищення особистих даних. Ці атаки, засновані на даних, швидко стають однією з найнебезпечніших проблем конфіденційності для конфіденційності даних в світі, оскільки багато платформ електронної комерції як і раніше працюють з SQL-запитами для інвентаризації та обробки замовлень. Загалом, одна вдало розміщена SQL-ін'єкція може коштувати компанії мільйони (або навіть мільярди, якщо ваша компанія така ж велика, як Apple або Amazon).
   1. Загальновідомі інциденти порушення безпеки функціонування корпоративних мереж.
10. WannaCry - наймасовіший вірус десятиліття.

WannaCry - шкідлива програма-вимагач, яка використовувала уразливість нульового дня в різних версіях Windows. Проникаючи в комп'ютери, вірус зашифровував весь вміст, а потім починав вимагати гроші за розблокування. Однак розшифрувати файли було неможливо. На рис. 1.1 зображено вікно з вимогами вимагачів WannaCry.



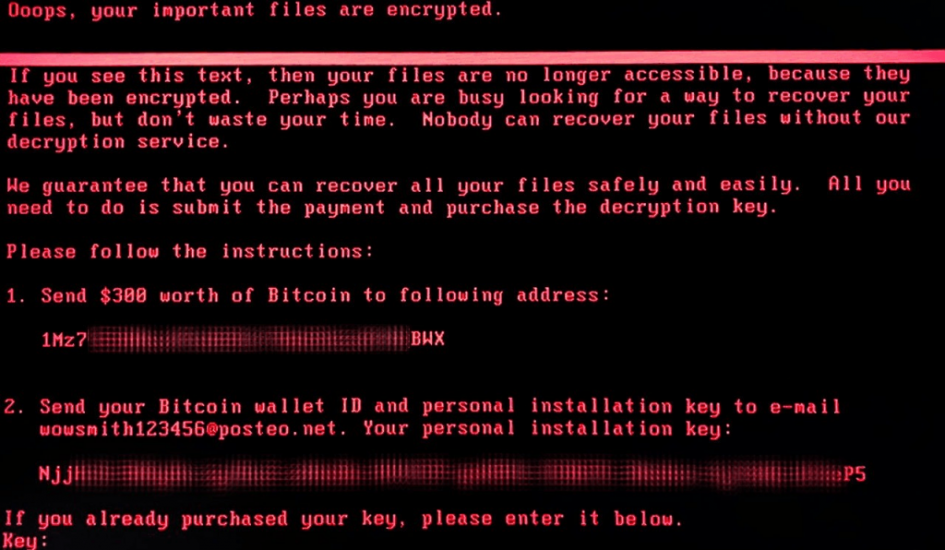
Рисунок 1.1 - Вікно з вимогами вимагачів WannaCry.

Вперше його виявили в Іспанії, а потім і в інших країнах. Найбільше постраждали Росія, Україна і Індія. Через WannaCry зупинилася робота банків, урядових організацій, аеропортів. У ряді британських лікарень не змогли провести термінові операції. Код вірусу виглядав занадто примітивним і начебто недописаним. Тому з'явилися версії, що розробник випадково випустив його завчасно. На користь цього говорить і те, що коди для розшифровки не працювали. Припускають, що спочатку WannaCry повинен був вразити всі пристрої на Windows. Зупинити вірус вдалося досліднику Маркусу Хатчинсі під ніком Malwaretech. Він звернув увагу, що перед тим, як зашифрувати файли, програма відправляє запит на неіснуючий домен. Хатчинс зареєстрував цей домен, після чого WannaCry перестав завдавати шкоди. У створенні вірусу підозрюють Lazarus Group та інші угруповання, пов'язані з Агентством національної безпеки США: дані про уразливість були відомі тільки АНБ.

1. Petya / NotPetya / ExPetr - найбільший збиток від кібератаки.

Перша версія вірусу з'явилася ще в березні 2016 року, але серйозні кібератаки почалися в 2017. Не всі згодні з тим, що в обох випадках це був один і той же вірус, але значна частина коду дійсно збігалася. Так само, як і WannaCry, Petya і його пізні версії вражали комп'ютери на ОС Microsoft Windows. Вони зашифровували файли - точніше, базу даних з інформацією про всі файли на диску - і дані для завантаження ОС. Потім вірус вимагав викуп у біткоінах. На рис. 1.2 зображено екран ураженого вірусом NotPetya комп’ютера.

Рисунок 1.2 – Екран ураженого вірусом NotPetya комп’ютера.



Але коди для розшифровки не допомагали, а, навпаки, знищували все дані на жорсткому диску. При цьому вірус отримував повний контроль над усією інфраструктурою компанії, і захист від WannaCry проти нього вже не діяла. Для створення NotPetya використовували коди хакерського угруповання Equation, викладені у відкритий доступ. У жовтні 2020 влада США звинуватила хакерську угруповання Sandworm, що складається із співробітників російського ГРУ, в причетності до вірусу NotPetya і інших кібератак. Найбільше від вірусу постраждала Україна. Пізніше прийшли до висновку, що саме звідси почалося зараження. Причина - в автоматичному оновленні бухгалтерської програми M.Е.Doc, якою користується більшість компаній і держорганів в країні.

1. Вибори в США - головний політичний скандал.

Хакери використовували шкідливе ПО для віддаленого управління серверами і передачі файлів, а також стеження за всіма діями користувачів в рамках мережі. Після кібератаки хакери вичистили всі сліди своєї активності. Хакерам вдалося отримати доступ до електронної пошти кандидата в президенти від демократів Хіларі Клінтон та її команди. В результаті 30 тис. Електронних листів були опубліковані на WikiLeaks, включаючи 7,5 тис. документів, відправлених самій Клінтон. Багато документів були секретними і стосувалися терористичних атак на консульство США в Бенгазі в 2012 році. Решта містили персональні дані членів і спонсорів демократичної партії, включаючи номери їх кредитних карт. Американські експерти з інтернет-безпеки звинуватили в цих атаках діючі з Росії хакерські угрупування під назвою Cozy Bear і Fancy Bear.

1. Злом Facebook - найгучніший витік даних з соцмережі.

У березні 2020 року британська компанія Comparitech повідомила про витік даних більш 267 млн ​​користувачів Facebook. Велика частина з них належить американцям. Їх могли використовувати для розсилки фішингових посилань. У серпні 2020 року експерти з компанії DarkNet Data Leakage & Breach Intelligence (DLBI) виявили в Мережі персональні дані 150 млн користувачів Facebook, Instagram і LinkedIn. На цей раз дані викрали з сервера в США, який належить китайській компанії Shenzhen Benniao Social Technology (socialarks.com). Вона продає рекламу і просування в соціальних мережах. Після перших витоків Федеральна торгова комісія США зобов'язала Facebook виплатити рекордні $ 5 млрд штрафу. Це в 20 разів вище найбільших санкцій, які застосовувалися за витік даних. Репутація самої компанії на тлі регулярних витоків сильно похитнулася - як і позиції на фондовій біржі.

1. Гучній злом акаунтів знаменитостей в Twitter.

У зламаних профілях зловмисники, від імені американських зірок, політиків і бізнесменів, закликали відправляти біткоіни на вказаний криптогаманець. Кожен переказ вони обіцяли повернути в подвійному розмірі. Постраждали також корпоративні акаунти Apple і Uber. Приклади зламаних акаунтів зображено на рисунку 1.3.



Рисунок 1.3 – Приклади зламаних акаунтів

1. Stuxnet - найперша кіберзброя.

Мережевий вірус Win32 / Stuxnet вразив особисті комп'ютери, а також цілі автоматизовані системи управління виробництвом. Він використовував чотири уразливості «нульового дня» в ОС Windows, перехоплюючи і змінюючи потік даних промислових підприємств, електростанцій та аеропортів. На рисунку 1.4 зображено як розповсюджувався Stuxnet.

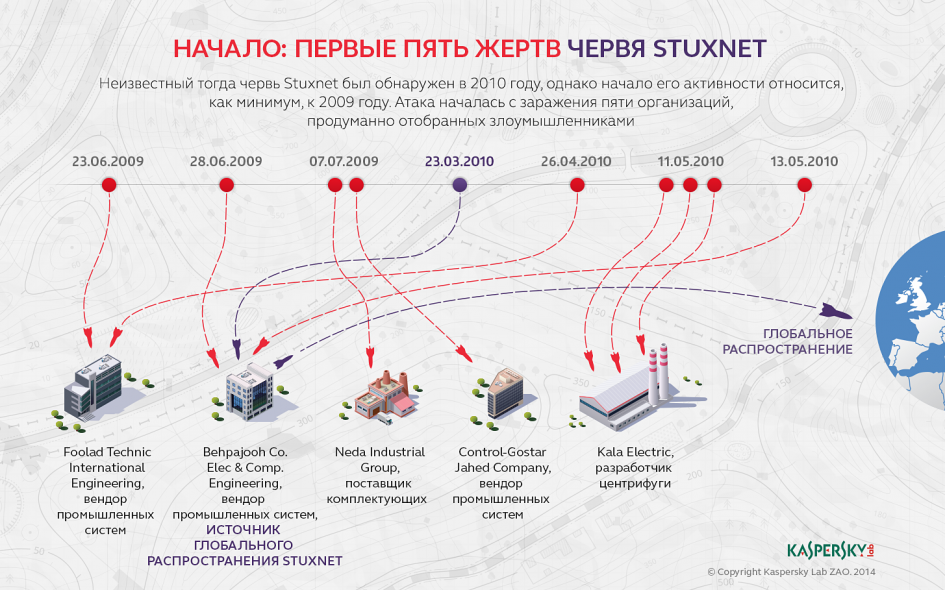


Рисунок 1.4 – Як розповсюджувався Stuxnet

У коді фахівці знайшли сліди програми уразливості «нульового дня», явно написаної професіоналами. З'явилися версії, що Stuxnet був запущений з конкретною метою - атакувати блоки управління газовими центрифугами для отримання збагаченого урану на стратегічних об'єктах. Саме заводи, які їх випускали, стали ще однією мішенню шкідливого ПЗ. Зловмисники розраховували, що від них вірус пошириться на заводи з виробництва збагаченого урану в Ірані, щоб нанести удар по всьому ядерному проекту. Їх план спрацював. У підсумку головними підозрюваними в кібератаці стали спецслужби Ізраїлю і США. The New York Times писала, що перед запуском Stuxnet був успішно випробуваний в ізраїльському місті Дімона в пустелі Негев. Журналістка Кім Зеттер присвятила цій події книгу «Зворотний відлік до нульового часу» (Countdown to zero day).

1. Yahoo - наймасштабніший витік даних.

Зловмисники зламали акаунти користувачів Yahoo і вкрали їх особисті дані, включаючи адреси електронної пошти і номери телефонів. Злочинці діяли в два етапи - в 2013 і 2014 роках, при цьому Yahoo розповіла про це тільки в 2016-му. Відповідальність за кібератаку була покладена на двох співробітників ФСБ і двох хакерів з Росії і Канади. З них тільки канадець визнав свою провину і отримав п'ять років в'язниці.

1. Marriott - найсерйозніший удар по репутації.

У 2014 році хакери зламали систему Starwood Preferred Guest, де зберігалися дані про клієнтів готелів Marriott: імена і прізвища, номери паспортів, контактні та платіжні дані. Атака розкрилася лише чотири роки по тому. Підозри впали на угруповання з числа співробітників китайської розвідки, яка намагалася зібрати дані про громадян США.

1. BlueLeaks - найгучніший витік даних з держорганів.

Хакери з угруповання Anonymous отримали доступ до 269 Гб секретних даних правоохоронних органів і спецслужб США у вигляді більш 1 млн файлів: відеоролики, електронні листи, аудіофайли, а також документи з планування та розвідки за останні десять років - включаючи ті, що підтверджують стеження за активістами Black Lives Matter. Файли передали групі хакерів-активістів DDoSecrets [30], яка опублікувала отриману інформацію. У відповідь на це Twitter заблокував акаунт DDoSecrets, а в Німеччині заблокували сервер, на якому зберігалися дані BlueLeaks - за запитом від американської влади.

До речі, в січні 2019 року теж саме ж угрупування опублікувало 175 Гб даних про таємні угоди Кремля, Російської православної церкви і участі Росії у війні на Донбасі.

1. Найскандальніша кібератака російських хакерів.

Хакери спробували зламати поштові сервери АНБ. Зловмисники використовували вразливість у агента пересилання повідомлень Exim, виявлену в червні 2019 року. Вона дозволяє злочинцеві відправляти шкідливе лист на сервер і відразу ж отримувати можливість віддалено запускати там же свій код. АНБ звинуватила в атаці хакерське угруповання Sandworm (вона ж - Telebots, Voodoo Bear, Iron Viking і BlackEnergy), пов'язану з Росією - ту саму, яка, ймовірно, запустила вірус NotPetya. Її ж Мін'юст США пізніше звинуватив в причетності до політичних подій в Грузії і на Україні, а також у втручанні в вибори у Франції та атаці на комп'ютерну мережу Зимових Олімпійських ігор в Пхенчхані в 2018 році.

* 1. Основні методи та засоби захисту корпоративних мереж.

Способи захисту інформації на підприємстві, також як і способи її видобутку, постійно змінюються. Регулярно з'являються нові пропозиції від компаній, що надають послуги із захисту інформації. Панацеї звичайно немає, але є кілька базових кроків побудови захисту інформаційної системи підприємства, на які обов'язково потрібно звернути увагу.

Багатьом напевно знайома концепція глибокої захисту від злому інформаційної мережі. Основна її ідея полягає в тому, щоб використовувати кілька рівнів оборони. Це дозволить, як мінімум, мінімізувати збитки, пов'язані з можливим порушенням периметра безпеки інформаційної системи.

Далі мною розглянуто загальні аспекти комп'ютерної безпеки.

1. Брандмауер (файрвол, брендмауер).

Брандмауер або файрвол - це перша лінія оборони, яка зустрічає непрошених гостей.

За рівнем контролю доступу виділяють наступні типи брендмауера:

* У найпростішому випадку фільтрація мережевих пакетів відбувається відповідно до встановлених правил, тобто на основі адреси джерела і призначення мережевих пакетів, номерів мережевих портів;
* Брєндмауер, що працює на сеансовому рівні (stateful). Він відстежує активні сполуки і відкидає підроблені пакети, що порушують специфікації TCP / IP;
* Файрвол, що працює на прикладному рівні. Виробляє фільтрацію на основі аналізу даних програми, що передаються всередині пакету.

Підвищена увага до мережевої безпеки і розвиток електронної комерції призвело до того, що все більше число користувачів використовують для свого захисту шифрування з'єднань (SSL, VPN). Це досить сильно ускладнює аналіз трафіку що проходить через міжмережеві екрани. Як можна здогадатися, тими ж технологіями користуються розробники шкідливого програмного забезпечення. Віруси, які використовують шифрування трафіку, практично не відрізняються від легального трафіку користувачів.

1. Віртуальні приватні мережі (VPN).

Ситуації, коли співробітнику необхідний доступ до ресурсів компанії з громадських місць (Wi-Fi в аеропорту або готелі) або з дому (домашню мережу співробітників не контролюють адміністратори), особливо небезпечні для корпоративної інформації. Для їх захисту просто необхідно використовувати шифровані тунелі VPN. Ні про який доступ до віддаленого робочого столу (RDP) безпосередньо не використовує шифрування даних, не може бути й мови. Це ж стосується використання стороннього ПЗ: Teamviewer, Aammy Admin і т.д. для доступу до робочої мережі. Трафік через ці програми шифрується, але проходить через непідконтрольні вам сервера розробників цього ПО.

До недоліків VPN можна віднести відносну складність розгортання, додаткові витрати на ключі аутентифікації і збільшення пропускної здатності інтернет каналу. Ключі аутентифікації також можуть бути скомпрометовані. Вкрадені мобільні пристрої компанії або співробітників (ноутбуки, планшети, смартфони) з попередньо налаштованими параметрами підключення VPN можуть стати потенційною діркою для несанкціонованого доступу до ресурсів компанії.

1. Системи виявлення й запобігання вторгнень (IDS, IPS).

Система виявлення вторгнень (IDS - англ .: Intrusion Detection System) - програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу до комп'ютерної системи (мережі), або несанкціонованого управління такою системою. У найпростішому випадку така система допомагає виявити сканування мережевих портів вашої системи або спроби увійти на сервер. У першому випадку це вказує на первинну розвідку зловмисником, а в другому спробу злому вашого сервера. Також можна виявити атаки, спрямовані на підвищення привілеїв в системі, неавторизований доступ до важливих файлів, а також дії шкідливого програмного забезпечення. Просунуті мережеві комутатори дозволяють підключити систему виявлення вторгнень, використовуючи віддзеркалення портів, або через отвітвитель трафіку.

Система запобігання вторгнень (IPS - англ .: Intrusion Prevention System) -програмні або апаратна система забезпечення безпеки, активно блокує вторгнення в міру їх виявлення. У разі виявлення вторгнення, підозрілий мережевий трафік може бути автоматично перекритий, а повідомлення про це негайно відправлено адміністратору.

1. Антивірусний захист.

Антивірусне програмне забезпечення є основним рубіжем захисту для більшості сучасних підприємств. За даними дослідницької компанії Gartner, обсяг ринку антивірусного ПО за підсумками 2012 року склав $ 19,14 млрд. Основні споживачі - сегмент середнього і малого бізнесу.

Перш за все антивірусний захист націлений на клієнтські пристрої та робочі станції. Бізнес-версії антивірусів включають функції централізованого управління для передачі оновлень антивірусних баз клієнтських пристроїв, а також можливість централізованого налаштування політики безпеки. В асортименті антивірусних компаній присутні спеціалізовані рішення для серверів.

З огляду на те, що більшість заражень шкідливим ПО відбувається в результаті дій користувача, антивірусні пакети пропонують комплексні варіанти захисту. Наприклад, захист програм електронної пошти, чатів, перевірку відвідуваних користувачами сайтів. Крім того, антивірусні пакети все частіше включають в себе програмний брандмауер, механізми проактивного захисту, а також механізми фільтрації спаму.

1. Білі списки.

Що з себе представляють "білі списки"? Існують два основні підходи до інформаційної безпеки. Перший підхід передбачає, що в операційній системі за замовчуванням дозволено запуск будь-яких додатків, якщо вони раніше не внесені до "чорного списку". Другий підхід, навпаки, передбачає, що дозволений запуск тільки тих програм, які заздалегідь були внесені до "білого списку", а всі інші програми за замовчуванням блокуються. Другий підхід до безпеки звичайно більш кращий в корпоративному світі. Білі списки можна створити, як за допомогою вбудованих засобів операційної системи, так і за допомогою стороннього ПО. Антивірусне ПЗ часто пропонує дану функцію в своєму складі. Більшість антивірусних програм, що пропонують фільтрацію по білому списку, дозволяють провести первинне налаштування дуже швидко, з мінімальним увагою з боку користувача.

Проте, можуть виникнути ситуації, в яких залежно від файлів, програми з білого списку були правильно визначені вами або антивірусним ПЗ. Це призведе до збоїв програми або до неправильного його встановлення. Крім того, білі списки безсилі проти атак, що використовують уразливості обробки документів програмами з білого списку. Також слід звернути увагу на найслабшу ланка в будь-якому захисті: самі співробітники в поспіху можуть проігнорувати попередження антивірусного ПО і додати в білий список шкідливе програмне забезпечення.

1. Фільтрація спаму.

Спам розсилки часто застосовуються для проведення фішинг атак, що використовуються для впровадження трояну або іншого шкідливий забезпечення в корпоративну мережу. Користувачі, які щодня обробляють велику кількість електронної пошти, більш сприйнятливі до фішинг-повідомленнями. Тому завдання ІТ-відділу компанії - відфільтрувати максимальну кількість спаму із загального потоку електронної пошти.

Основні способи фільтрації спаму:

* Спеціалізовані постачальники сервісів фільтрації спаму;
* ПО для фільтрації спаму на власних поштових серверах;
* Спеціалізовані хардварні рішення, розгорнуті в корпоративному дата-центрі.

1. Підтримка ПО в актуальному стані.

Своєчасне оновлення програмного забезпечення і застосування актуальних оновлень безпеки - важливий елемент захисту корпоративної мережі від несанкціонованого доступу. Виробники ПЗ, як правило, не надають повну інформацію про нові знайдені діри в безпеці. Однак зловмисникам вистачає і загального опису уразливості, щоб буквально за пару годин після публікації опису нової дірки, написати програмне забезпечення для експлуатації цієї уразливості.

Насправді це досить велика проблема для підприємств малого та середнього бізнесу, оскільки зазвичай використовується широкий спектр програмних продуктів різних виробників. Часто оновленням всього парку ПО не приділяється належної уваги, а це практично відкрите вікно в системі безпеки підприємства. В даний час велика кількість ПО самостійно оновлюється з серверів виробника і це знімає частину проблеми. Чому частина? Тому що сервера виробника можуть бути зламані і, під виглядом легальних оновлень, ви отримаєте свіже шкідливе ПЗ. А також і самі виробники часом випускають оновлення, що порушують нормальну роботу свого ПО. На критично важливих ділянках бізнесу це неприпустимо. Для запобігання подібних інцидентів всі отримувані поновлення, по-перше, повинні бути застосовані відразу після їх випуску, по-друге, перед застосуванням вони обов'язково повинні бути ретельно протестовані.

1. Фізична безпека.

Фізична безпека корпоративної мережі є одним з найважливіших факторів, який складно переоцінити. Маючи фізичний доступ до мережних пристроїв зловмисник, в більшості випадків, легко отримає доступ до вашої мережі. Наприклад, якщо є фізичний доступ до комутатора і в мережі не проводиться фільтрація МАС-адрес. Хоча і фільтрація MAC в цьому випадку вас не врятує. Ще однією проблемою є крадіжка або недбале ставлення до жорстких дисків після заміни в сервері або іншому пристрої. З огляду на те, що знайдені там паролі можуть бути розшифровані, серверні шафи і кімнати або ящики з обладнанням повинні бути завжди надійно захищені від проникнення сторонніх.

Важливо також звернути увагу на навчання користувачів, періодичний незалежний аудит інформаційної безпеки, створення і дотримання надійної політики інформаційної безпеки.

Захист корпоративної мережі є досить складною темою, яка постійно змінюється. Потрібно бути впевненим, що компанія не залежить лише від одного-двох рубіжів захисту. Завжди є потреба стежити за актуальною інформацією і свіжими рішеннями на ринку інформаційної безпеки.

1. АНАЛІЗ ВІДОМИХ МЕТОДИК ТЕСТУВАННЯ
   1. OWASP Testing Guide

Проект OWASP розроблявся протягом багатьох років. Мета проекту - допомогти людям зрозуміти, що, чому, коли, де і як тестують веб-програми. Проект забезпечив повний цикл тестування, а не просто простий контрольний перелік чи припис питань, які слід вирішити. Читачі можуть використовувати цей фреймворк як шаблон для побудови власних програм тестування або для кваліфікації процесів інших людей. OWASP Testing Guide докладно описує як загальну основу тестування, так і методи, необхідні для реалізації основи на практиці.

Написання посібника з тестування виявилось складним завданням. Було викликом отримати консенсус та розробити контент що дозволив людям застосовувати концепції, описані в посібнику, одночасно дозволяючи їм працювати самостійно. Також було проблемою змінити фокус тестування веб-додатків з тестування на проникнення до тестування, інтегрованого в життєвий цикл розробки програмного забезпечення.

Однак група дуже задоволена результатами проекту. Багато галузевих експертів та фахівців з безпеки, деякі з яких відповідають за безпеку програмного забезпечення в деяких найбільших компаніях у світі, перевіряють рамки тестування. Цей фреймворк допомагає організаціям тестувати свої веб-програми для створення надійного та безпечного програмного забезпечення.

Решта посібника організована таким чином: цей вступ охоплює передумови тестування веб-додатків та обсяг тестування. Він також охоплює принципи успішного тестування та техніки тестування, найкращі практики для звітування та бізнес-кейси для перевірки безпеки. Розділ 3 представляє структуру тестування OWASP та пояснює її техніки та завдання стосовно різних фаз життєвого циклу розробки програмного забезпечення. Розділ 4 висвітлює, як зробити перевірку специфічних вразливостей (наприклад, SQL Injection) шляхом перевірки коду та тестування на проникнення.

На початку керівництва по тестуванню від OWASP є невелика передмова, з якого випливає, що автоматизоване Black Box тестування має недоліки і його треба доповнювати ручним тестуванням. Це так, проте в самому тексті гайду зустрічаються різні приклади використання сканера Nessus, але немає ні слова про сканер OpenVas, який, в принципі, не сильно гірше.

Має сенс використовувати всі наявні сканери та інші фічі платних продуктів (наприклад, burp pro), оскільки різні інструменти можуть дати різні результати. Не треба зневажати хибнопозитивні спрацьовуванн, оскільки такі результати іноді раптово виявляються істинними.

Основні пункти OWASP Testing Guide:

1. Conduct search engine discovery / reconnaissance for information leakage

Збір інформації з відкритих джерел (OSINT) - перший етап будь-якого пентеста, в тому числі, і пентеста веб-додатки. Цей етап проводиться ще до початку робіт, щоб перевірити, чи дійсно тестовані об'єкти належать замовнику, або щоб оцінити приблизний обсяг робіт для оцінки трудовитрат. У методології цей етап в основному будується на використанні пошукових движків (причому різних, щоб компенсувати обмеження одного перевагами іншого). Тут на допомогу прийде стаття, що описує можливості DuckDuckGo, замітка про оператори пошуку і google dorks. Але, зрозуміло OSINT не обмежується тільки лише використанням пошуку, як мінімум через наявність неіндексований форумів, в тому числі, в даркнеті, або персоналізованої видачі. До речі, на будь-якому етапі тестування не варто забувати про персоналізованої видачі самого тестованого ресурсу. Можна використовувати різні техніки пасивного збору інформації, в тому числі, такий інструмент, як FOCA для отримання метаданих з документів, які швидше за все присутні на тестованих ресурсах. Не варто забувати про сайти, прямо або побічно пов'язані з IT, а також тематичні (щодо тематики тестованого об'єкта) ресурси. Загалом, про OSINT можна говорити довго, суть в тому, що треба використовувати керівництво по тестуванню, як основу, а не як покрокову інструкцію.

1. Map execution paths through application. Тут йдеться про складання «карти» веб-додатки, тобто, про відображення в текстовому або графічному вигляді всіх або майже всіх розділів сайту. Якщо цей процес автоматизувати за допомогою відповідних інструментів, то можна отримаєш схему веб-додатку або сайту, на яку можна спиратися при тестуванні. Наприклад, така схема допоможе класифікувати рубрики сайту по розділах методології. До того ж, автоматизовані утиліти можуть виявити те, що було не знайдено на етапі збору інформації.
2. Configuration and Deployment Management Testing. У цьому розділі описано тестування інфраструктури веб-додатки. У гайді мова йде в основному про веб-сервери і СУБД. І хоч це фундамент будь-якого веб-додатки, не варто забувати про CI / CD-системи, шини повідомлень та інші компоненти інфраструктури. Звичайно, якщо вони входять в намічений план робіт.
3. Authentication testing / Authorization testing. При тестуванні аутентифікації і авторизації не варто забувати про такі речі, як OAuth, SSO, OpenID. Навіть може зустрітися аутентифікація за сертифікатами.
4. Input validation testing. Перші два пункти цього розділу пов'язані з reflected / stored XSS-уразливими. Але XSS-уразливість є підкласом більш загальних вразливостей - reflected / stored HTML injection. Може трапитися так, що XSS немає, а ось HTML injection є. До речі, крім XSS / HTML-ін'єкцій також не треба забувати про ін'єкції в шаблонах - досить серйозний підклас атак, який може привести до віддаленого виконання коду. Ще одним підвидом атаки віддаленого виконання коду є атака SSRF.

Також не варто забувати про те, в якому оточенні працює веб-додаток. Потрібно подумати про те, як потенційний зловмисник може використовувати це для своєї вигоди. У 7 розділі також йдеться про бінарні уразливості Overflow і Format String: сюди взагалі варто включити весь спектр бінарних вразливостей зі всілякими хитрощами, які можна здійснити віддалено.

1. Business logic testing. Взагалі, в розділ, присвячений тестуванню бізнес логіки, можна включити все, що завгодно. Проблеми в цій сфері можуть призвести до можливості DDOS-атаки, порушення цілісності, конфіденційності та доступності інформації, і т.д. Варіантів можна придумати безліч, тут суть не в тому, щоб передбачити всі можливі варіанти, а в тому, щоб навчитися діяти по ситуації. Тому цей розділ носить в основному теоретичний характер: практичні прийоми тестування залежать від архітектури і внутрішнього устрою конкретного досліджуваного об'єкта.
2. Client side testing. У перших двох пунктах цієї частини керівництва мова знову заходить про XSS-уразливість, але на стороні клієнта. Тут слід звернути увагу на дві обставини. По-перше, не варто забувати про HTML injection (її теж можна здійснити на стороні клієнта). По-друге, XSS-уразливість діляться на 4 типи: server-side reflected, server-side stored, client-side reflected, і client-side stored. В останньому випадку в якості сховища для XSS-навантаження використовується сховище браузера (в межах сесії або ж на довший термін). На мій погляд, розподіл має бути саме по client-side reflected і client-side stored, бо атаки DOM-based XSS і arbitrary JS injections можуть бути виконані в контексті обох вищезазначених вразливостей. Аналогічно, родичем атаки SSTI (server side template injection) є CSTI. Принцип її той же самий, але здійснюється вона на боці клієнта.
   1. NIST Special Publication 800-42 Guideline on Network Security Testing