УДК 004.725.5
DOI: 10.31673/2409-7292.2020.023236

Маслов О.Г., Кітура О.В.

МЕТОДИКА ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ІНТЕРНЕТ РЕЧЕЙ НА БАЗІ ТЕХНОЛОГІЙ БЛОКЧЕЙНА

Показані шляхи несанкціонованого отримання інформації у інформаційно-телекомунікаційних системах. Показані три етапи процесу запобігання або зниження ризиків небезпек в інформаційно-телекомунікаційних системах. Розглянуто загрози інформаційній безпеці у інформаційно-телекомунікаційних системах, та їх класифікація. Приведені методи та технології протидії загрозам інформації в інформаційно-телекомунікаційних системах.. Зроблено висновок про необхідність моніторингу нових технологічних рішень для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

Ключові слова: локальна мережа, інформаційно-телекомунікаційна система, інформація з обмеженим доступом, об'єкт інформаційної діяльності, інформаційна безпека, конфіденційність.

Вступ

Локальні мережі комп'ютерних систем охоплюють багато сфер людської діяльності. Така їх популярність породжує задачі пов'язані із захистом інформації у них. Ці питання є невід'ємною частиною любої мережі у якій є комерційна або конфіденційна інформація. Використанні Internet у приватних межах, а також з'єднання розосереджених частин компаній і організацій породжує проблему. Це – безпека інформації у мережі.

Основна частина.

Технологія функціонування локальної обчислювальної мережі (ЛОМ) та її архітектура дає змогу порушнику винаходити все більш оригінальні способи для несанкціонованого доступу до інформації. Опираючись на відомі різноманітні факти злочинних дій, ми можемо припустити, що лазівок для прихованого доступу існує достатньо. Шляхи несанкціонованого отримання інформації у ЛОМ наведені на рис. 1.1.

Рис. 1. Шляхи несанкціонованого отримання інформації

Відповідно до рис. 1.1 бувають непрямі та прямі шляхи доступу до даних ЛОМ [1].

Для застосування прямих потрібен безпосередній доступу до елементів ЛОМ. Непрямі цього не потребують.

До дуже поширених шляхів несанкціонованого отримання інформації відносяться. Підслуховуючі пристрої, перехоплення випромінювань засобів обробки інформації, крадіжка матеріальних носіїв секретної інформації. Крім того активно застосовуються приховування

під зареєстрованого користувача, програмні пастки, недолікі мов програмування і операційних систем, замасковане підключення до апаратури чи ліній зв'язку обчислювальної системи ін.

Взагалі процес запобігання або зниження ризиків небезпек обчислювальній системі складається з трьох етапів:

- класифікація загроз інформаційній безпеці системи;
- визначення методів захисту від загроз інформаційній безпеці;
- визначення технології захисту.

Стосовно класифікації загроз.

Співробітники Майкрософт розробили, обґрунтували та активно посувають на міжнародному рівні методику STRIDE [2]. Вона являє собою класифікацію загроз за їхніми наслідками. STRIDE потрібна при побудові моделі загроз при розробці програмного забезпечення. Така назва (STRIDE) виникла з перших букв назв загроз [2]. А саме.

*Підміна об'єктів [**S**poofing identity], Модифікація даних [**T**ampering with data], Відмова від авторства [**R**epudiation of origin], Розголошення інформації [**I**nformation disclosure], Відмова в обслуговуванні [**D**eniai of service], Підвищення привілеїв [**E**levation of privilege].*

Стосовно визначення методів та технологій захисту від загроз інформаційній безпеці необхідно відмітити наступне. При створенні системи кібербезпки, застосовуються наступні засоби:

Технічні. Вони складаються з:

- апаратних. Пристрої, що являють одне ціле з апаратурою ЛОМ. Обмін даними здійснюється по стандартному інтерфейсу. Можуть бути наприклад міжмережеві екрани тощо;
- фізичні. Це спеціальні автономні пристрої та системи. Як приклад можна віднести охоронно-тривожну сигналізацію, відео системи, біометрика на дверях, решітки на вікнах.
- програмні. Використовується особливе програмне забезпечення для захисту інформації.

Спеціалісти кібербезпеки, зважаючи на розвиток концепції захисту інформації, зробили висновок. Він пояснює що застосування одного з вище показаних способів не може гарантувати надійний кіберзахист. Потрібен багатовекторний підхід для поєднання всіх засобів і способів для нідійної кібербезпеки. Вектори забезпечення кібербезпеки є на рисунку 1.2.

Рисунок 2. Способи і засоби захисту інформації в ЛОМ

Реалізація векторів кібербезпеки на визначеному певному рівні моделі OSI вимагає застосування відповідних механізмів [3]. Це шифрування, електронний цифровій підпис, моніторінг цілісності даних, автентифікаційний обмін даними, заповнення трафіку ін.

Виходячи з наведеного пропонується поетапний методичний підхід для побудови ефективно захищеної ЛОМ підприємства.

Етап 1 (безпека інфраструктури) дозволяє зрозуміти, що знаходиться у вашій мережі, і визначає базові вимоги щодо інформаційної безпеки.

Етап 2 (навчання співробітників) приділяє основну увагу забезпеченню базових вимог безпеки і навчання співробітників питань інформаційної безпеки.

Етап 3 (реакція на інциденти) допомагає організації підготуватися до інцидентів з інформаційної безпеки.

Етап 1. Безпека інфраструктури

На самому початку, щоб просунутися в питанні інформаційної безпеки, необхідно розібратися з локальною мережею, підключеними пристроями, критично важливими даними та програмами. Без чіткого розуміння того, що вам потрібно захистити, вам буде важко переконатися в тому, що ви забезпечуєте прийнятний рівень інформаційної безпеки.

Ключові питання, які необхідно тримати в голові:

1) Розібратись яку інформацію необхідно захищати?
2) Де у мережі зберігається найважливіша інформація?
3) Знати які пристрої підключені до мережі?
4) Яке програмне забезпечення встановлено на комп'ютерах співробітників?
5) Чи використовують системні адміністратори і користувачі надійні паролі?
6) Які онлайн-ресурси використовують співробітники (тобто Працюють або сидять в соціальних мережах)?

Де у мережі зберігається найважливіша інформація. Можливі великі неприємності організації, якщо критично важливі дані її будуть втрачені, викрадені або ушкоджені. Випадкові події та природні катаклізми також можуть завдати непоправної шкоди. Крім того, потенційні зловмисники націлені на дані, які можуть мати цінність для них. Щоб захистити своє підприємство, необхідно розуміти цінність даних і як їх можна використовувати.

Якщо є розуміння які пристрої підключені до мережі, то інфраструктура стає простіше в управлінні. Наприклад якщо є бездротова мережа, потрібно перевірити на маршрутизаторі які пристрої підключені, і чи застосовується надійне шифрування. Необхідно увімкнути логування подій, пов'язаних з підключенням мережевих пристроїв, які отримують ір-адреса по протоколу DHCP. Це забезпечить зручне відстеження всіх пристроїв, які були у вашій мережі.

Шкідливе програмне забезпечення (ПЗ) на комп’ютерах співробітників може створювати ризики, які необхідно мінімізувати. Неоновлене програмне забезпечення є поширеною причиною проникнення шкідливого ПЗ, яке призводить до атак на інформаційні системи. Якщо є розуміння, яке програмне забезпечення встановлено у мережі та захист облікових записів з правами адміністратора, то зменшується ймовірність і вплив інцидентів інформаційної безпеки. Для цього потрібно створити перелік додатків, веб-сервісів або хмарних рішень, які використовує ваша організація. Обмежити число користувачів з правами адміністратора до мінімально можливого значення. Не дозволяти звичайним користувачам працювати в системі з правами адміністратора. Використовувати складні паролі для адміністративних облікових записів, так як адміністратори можуть вносити серйозні зміни в систему. Розробити інструкцію для співробітників зі складання складних паролів.

Переконатися, що системні адміністратори використовують окремий не призначений для користувача обліковий запис для читання електронної пошти, доступу в Інтернет і складання документів.

Захист інформації вимагає не тільки технологічних рішень, а й обізнаності співробітників про запобігання випадкового порушення роботи систем. В рамках цього етапу потрібно розуміння захисту комп'ютерів, і навчання співробітників важливим аспектам інформаційної безпеки.

Для отримання доступу в інформаційну систему шкідливі програми і зловмисники найчастіше використовують або небезпечно налаштовані додатки, або додатки з уразливостями. Необхідно переконатися, що операційна система і додатки (особливо веб-браузери) оновлені і правильно налаштовані. Також рекомендується використовувати механізми захисту від шкідливих програм, які можуть бути вбудовані в операційну систему. Наприклад, Windows Device Guard, Windows Bitlocker і інші.

Необхідно розуміння співробітниками організації своєї ролі у захисті секретної інформації.

Поширенішими атаками є фішингові атаки по електронній пошті і по телефону. Необхідно переконайтися, що співробітники можуть описати і визначити основні ознаки атаки. До таких ознак можуть відноситися ситуації, коли люди кажуть про терміновість, просять цінну або конфіденційну інформацію, використовують незрозумілі або технічні терміни, просять ігнорувати або обійти процедури безпеки. Необхідно заохочувати використання складних, унікальних паролів для кожного облікового запису і / або двухфактурну автентифікацію там, де це можливо. Вимагати від співробітників використовувати «блокування екрану» на своїх мобільних пристроях. Переконуватися, що всі співробітники постійно оновлюють свої пристрої і програмне забезпечення. По можливості поширювати серед співробітників безкоштовні інформаційні матеріали з питань інформаційної безпеки, такі як інформаційний бюлетень SANS OUCH і щомісячні інформаційні бюлетені MS-ISAC. Використовувати онлайн-ресурси, такі як Stay Safe Online.org Національного альянсу кібербезпеки.

Все вище перераховане дозволяє розробити серйозний фундамент з інформаційної безпеки. Далі необхідно вибудувати механізми реакції на інциденти. Такий підхід включає в себе розуміння, як справлятися з інцидентом інформаційної безпеки і як відновити роботу організації після нього.

Створення та управління резервними копіями це один з кращих способів захистити дані та відновитися після збою. Надійний план реагування, доповнений поточними і підтримуваними резервними копіями, є найкращим захистом при роботі з інцидентом з інформаційної безпеки. Для цього: автоматично виконувати щотижневі резервні копії всіх комп'ютерів з важливою інформацією. Періодично перевіряти свої резервні копії, відновлюючи систему з використанням резервної копії Переконуватися що, хоча б одна резервна копія недоступна по мережі. Для цього застосовується Microsoft утиліта резервного копіювання, вбудована в операційну систему Microsoft, Apple Time Machine - інструмент резервного копіювання, встановлений в операційних системах Apple. Інші інструменти.

До найпоширеніших інцидентів з кібербезпеки відносять атаку типу «відмова в обслуговуванні», яка порушує доступ до вашого сайту, атаку програм-вимагачів, які блокують вашу систему або ваші дані, атаку шкідливим ПЗ, яка призводить до втрати даних вашого клієнта або співробітника, а також крадіжку ноутбука, що містить незашифровані дані.

Попереджувальними заходами інциденту кібербезпеки можуть бути наступні. Потрібно визначити співробітників вашої організації, які будуть приймати рішення і давати вказівки в разі інциденту. Надати контактну інформацію для IT-персоналу та / або сторонніх організацій. Мати список зовнішніх контактів як частина плану. До них можуть відноситись юрисконсульти, страхові агенти, якщо застраховано ризики з інформаційної безпеки, консультанти з питань безпеки.

Комплексне рішення підвищення безпеки мережі.

Під комплексним підходом мається на увазі одне рішення, яке допоможе покращити та підвищити рівень інформаційної безпеки на всіх трьох етапах впровадження інформаційної

безпеки, описаних вище. Мається на увазі недороге вирішення основних проблем інформаційної безпеки на підприємстві. Це Data Loss Prevention (DLP) – система попередження втрат даних, як найбільш функціональне та доступне рішення - Symantec DLP [4].

Data Loss Prevention від Symantec - комплексне рішення забезпечення кібербезпеки, яке призначене для пошуку, моніторингу і захисту конфіденційної інформації з урахуванням її вмісту. Система складається з різних функціональних модулів.

Найбільшим плюсом, є вихід останнього оновлення програми, після якого Модулі Symantec Data Loss Prevention, включаючи сервер управління Enforce, модулі детектування і базу даних конфігурації та інцидентів тепер можна розгорнути на одному фізичному сервері, що значно знижує вимоги до кількості апаратного забезпечення при розгортанні системи в філіях або невеликих організаціях, а також знижує витрати на підтримку операційних

Висновок.

У статті проведено огляд існуючих загроз інформаційній безпеці у комп'ютерних мережах та методів і технологічних рішень протидії загрозам. Технологічні рішення бувають апаратної або програмної реалізації. Для забезпечення надійної кібербезпеки у ЛОМ необхідно поєднання апаратних, програмних та фізичних засобів. Розроблено рекомендації для забезпечення інформаційної безпеки ЛОМ на достатньому рівні.

Перелік посилань

1. Гайворонський М.В., Новіков К.А. Безпека інформаційно-комунікаційних систем / – К: Вид. група BHV, 2009. –608 с.

2. https:// https://docs.microsoft.com/ru-ru/azure/security/develop/threat-modeling-tool-threats [електронний ресурс].

3. Чаплигіна М.П. Показатели угроз безопасности модели OSI / - М: Молодий вчений, 2015. - № 13(93). – С. 214-217. – URL: https://moluch.ru/arhive/93\20668.

4. https:// https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/

Надійшла: 25.03.2020 Рецензент: д.т.н., доцент Кожухівський А.Д.