УДК 004.056.5

ІНФОРМАЦІЙНА БЕЗПЕКА ПІД ЧАС ВІДДАЛЕНОЇ РОБОТИ У ПЕРІОД КАРАНТИНУ

Матвієнко О. М., студ. гр. МКБп-191
Мехед Д. Б., к.пед.н, доцент кафедри кібербезпекки та математиного моделювання
Національний університет «Чернігівська політехніка»

З метою виявлення актуальних загроз інформаційної безпеки в умовах організації віддаленої роботи під час пандемії коронавирусу COVID-19 нами було досліджено IT компанії України за допомогою анонімного опитування їх співробітників. Отримані результати показали, що тільки 13% респондентів відмітили, що в їх компаніях було організовано віддалений доступ у зв'язку з карантином. Близько 80% респондентів розповіли, що в їх компаніях частина співробітників або навіть усі з них використовують для роботи домашні комп'ютери або ноутбуки. 57% респондентів відзначили, що не планують змінювати способи організації віддаленого доступу найближчим часом. Кожна п'ята компанія вивела на периметр корпоративні портали.

Виявилося, що повний або частковий віддалений доступ був організований в більшості компаній ще до карантину. Однак більш ніж половина респондентів зазначила, що його довелося екстрено організовувати з нуля (9%) або масштабувати на більшу кількість співробітників (71%). IT-компанії - лідер серед галузей по готовності до переходу на віддалену роботу: у 63% компаній віддалений режим роботи був організований ще до карантину. Для порівняння в телекомунікаційній сфері частка таких компаній становить 54%, у фінансовій - 46%, в промисловості - 32%, в ПЕК - 26%, в держструктурах - 24%.

Один з ризиків інформаційної безпеки при швидкому переході на віддалений режим роботи - є збільшення навантаження на IT-потужності і відсутність уважного моніторингу оновленої інфраструктури. Бажано, щоб співробітники працювали з доменних пристроїв, налаштованих за всіма стандартами безпеки. На них як мінімум повинні бути встановлені антивірусні засоби захисту і всі актуальні оновлення для ПЗ і ОС. Однак корпоративні ноутбуки видали далеко не всім. Співробітники 20% компаній працюють з робочих пристроїв, в інших 80% організацій частину або всі співробітники використовують домашні комп'ютери або ноутбуки. Найбільш безпечний варіант віддаленої роботи - використовувати виділені робочі пристрої.

На основі отриманих даних нами було створено ряд рекомендацій по організації віддаленої роботи в умовах карантину з метою забезпечення високого рівня інформаційної безпеки:

1. Організувати доступ до сервера управління корпоративними антивірусами на кінцевих вузлах через інтернет.

2. Забезпечити, щоб співробітники встановили у себе корпоративний антивірус і підключилися до сервера управління.

Це може повести за собою збільшення кількості ліцензій, але дозволить простіше поширити корпоративну політику безпеки на домашні пристрої. Також це дозволить порівнювати доменні адреси і простіше виявляти порушників і підозрілу активність.

У випадку організації віддаленої роботи компанії за допомогою VPN (як показало опитування, VPN користується найбільшою популярністю), слід заборонити роздільне тунелювання (split tunneling) та згорнути весь призначений для користувача трафік всередину інфраструктури через периметрові засоби захисту, наприклад проксі і NGFW. Інакше, якщо пристрій співробітника зламано і контролюється через інтернет, службі ІБ буде складно це виявити.

Пропускати трафік всіх користувачів через периметр приведе до навантаження на канали. Тому ми рекомендуємо сегментувати мережі і доступ до них, а через заборону

роздільного тунелювання обов'язково пропускати трафік співробітників, які працюють з конфіденційними даними.

Якщо заборонити роздільне тунелювання не виходить, то для забезпечення безпеки внутрішньої мережі знадобиться поведінковий аналіз. Наприклад, можна налаштувати повідомлення на випадки підключення співробітника з IP-адрес з інших країн або в неробочий час. Такі випадки можна покрити за допомогою SIEM-систем - дані в них збагачуються з додаткових джерел: GeoIP-сервісу і системи аналізу трафіку (NTA).

Якщо раніше для компаній більш актуальною був захист від зовнішніх загроз, то зараз самі користувачі систем стають зовнішньою загрозою. Тут як у випадку з коронавірусом - вийшов за двері, можеш повернутися зараженим і заразити інших. Користувачі перестають бути довіреною стороною при підключенні до інфраструктури.

Список використаних джерел

1. Тардаскін М.Ф. Технічний захист комерційної таємниці підприємства зв’язку: навч. посіб.; / за ред. М.В. Захарченка М.Ф. Тардаскін, В.Г. Кононович / – Одеса: ОНАЗ, 2002. – 76 с.

2. Тотальна війна і комп'ютерний soft, як її головний інструмент. [Електронний ресурс]. - Режим доступу: https://zillya.ua/totalna-viina-i-kompyuternii-soft-yak-golovnii-instrument.

3. Комп’ютерні мережі. [Електронний ресурс]. - Режим доступу:https://uk.wikipedia.org/wiki/Комп%27ютерна_мережа

4. Камалян А.К. Комп'ютерні мережі та засоби захисту інформації: Навчальний посібник / [А. К. Камалян, С. А. Кульов, К. М. Назаренко та ін.]. – Воронеж : (ВДАУ). 2003. – 119 с.

5. Концепція технічного захисту інформації в галузі зв’язку України. [Електронний ресурс]. - Режим доступу: http://zakon1.rada.gov.ua