УДК 004.62

Мінгальов В. Є. студент гр. 125м-20-2,
Мєшков В. І., старший викладач
(*Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна*)

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВІДДАЛЕНОГО РОБОЧОГО МІСЦЯ СПІВРОБІТНИКА КОМПАНІЇ

У зв'язку з пандемією COVID-19 на сьогоднішній день все більше людей отримують можливість працювати на компанію у віддаленому режимі, та все ширшим становиться потік конфіденційних даних які передаються між співробітниками та серверами обробки даних компаній. Раптовий перехід компанії у віддалений режим роботи, в обмеженому часі, досить суттєво поставив питання організації безпеки віддаленого робочого місця для співробітників.

Різні за знаннями у сфері безпеки інформації люди не завжди розуміють наскільки важливим є використання того чи іншого інструменту для безпечної обробки конфіденційних даних компанії у своїй роботі. Також домашні мережі майже завжди захищенні набагато менше, ніж мережі компанії, що потенційно може стати причиною багатьох проблем.

Безпека організації стає все більш залежною від обізнаності співробітників в питаннях інформаційної безпеки, тому рівень ризику несанкціонованого доступу до інформації (викриття, втрата, модифікація тощо) непомірно зростає.

Найбільш поширеними проблемами при віддаленій роботі вважаються: направлені дії з використанням методів соціальної інженерії, викриття паролів та конфіденційних даних, модифікація трафіка, фішинг та вплив на коректну роботу маршрутизаторів.

Серед популярних запропонованих методів для вирішення питання безпеки віддаленого робочого місця є використання:

- безпечного VPN-з'єднання для забезпечення захисту каналів зв'язку за допомогою яких відбувається обмін інформацією. Для цього будуть у нагоді програмні та апаратні VPN-продукти, наприклад: ExpressVPN, CyberGhost та Surfshark;
- засобів автентифікації, наприклад, технології багатофакторної автентифікації із використанням токенів, сертифікатів, відповідно налаштованих групових політик;
- засобів контролю витоків інформації та продуктивності співробітників, наприклад, завдяки використанню DLP (Data Leak Prevention)-систем, які дозволяють забезпечити контроль робочого місця поза офісом компанії та запобігати витоку інформації;
- хмарних захисних рішень, через високе навантаження на IT-інфраструктуру, підприємства змушені перерозподіляти потужності для забезпечення працездатність корпоративних ресурсів при віддалених підключеннях;
- систем контролю привілейованих користувачів, у зв'язку із переходом до віддаленого режиму не тільки звичайних користувачів, постає необхідність контролю того, які операції адміністратори виконуюсь над серверами та співробітники з привілейованим доступом – над критичними бізнес-системами;
- моделі захисту нульової довіри, що передбачає налаштування методів до захисту, ґрунтуючись повній недовірі до будь-яких користувачів, що намагаються підключитися до ресурсів компанії. Кожного разу під час підключення до ресурсів користувачі та пристрої повинні підтверджувати свою справжність.

Використання тих чи інших рішень не знаючи напевно потрібно воно насправді чи ні, а лише задля їх більшої кількості, не завжди допомагає збільшити рівень безпеки

інформації підприємства, тому що компанії можуть мати різну необхідність у вирішені конкретних питань інформаційної безпеки. Серед найбільш оптимальних по ціні та продуктивності є наступних алгоритм дій: обов'язкове регулярне проходження семінарів та курсів підвищення кваліфікації з кібербезпеки співробітником компанії, використання VPN для доступу до її внутрішніх ресурсів, виконання роботи тільки за допомогою корпоративних робочих станцій, контроль доступу до ресурсів у мережі Інтернет та використання ліцензованого програмного забезпечення, використання співробітником ресурсів компанії тільки за необхідності.

Перелік посилань

1. Кибербезопасность: проблемы и пути решения [Електронний ресурс] – Режим доступу до ресурсу: https://www.pitsasinsurances.com/ru/article/cyber-risk-problems-solutions-insurance/.

2. Корпоративный портал — оптимальное решение для организации рабочего места сотрудников [Електронний ресурс] – Режим доступу до ресурсу: https://www.top-personal.ru/sdeloissue.html?473.

3. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ ПРИ ВИРТУАЛИЗАЦИИ РАБОЧИХ СТОЛОВ [Електронний ресурс] – Режим доступу до ресурсу: https://applied-research.ru/ru/article/view?id=12968.

4. Безопасность удаленной работы: проблемы и рекомендации [Електронний ресурс] – Режим доступу до ресурсу: https://www.tadviser.ru/index.php/Статья:Безопасность_удаленной_работы:_проблемы_и_рекомендации.

5. Найкращі VPN 2021 року [Електронний ресурс] – Режим доступу до ресурсу: https://www.top10vpn.com/naykrashchyy-vpn/?bsid=c45se1kw102&gclid=EAIaIQobChMI-e6siO7q8wIVQ6OyCh2kNQwzEAAYASAAEgIXjfD_BwE.

6. Бизнес на расстоянии: как защитить инфраструктуру [Електронний ресурс] – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/knowledge-base/biznes-na-rasstoyanii-kak-zashchitit-infrastrukturu/.