УДК 004.031.6

ОРГАНІЗАЦІЯ БЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА

Волощук Р.Є. – гр. МгКІ-21, магістр, *VoloschukRostyslav@i.ua*
Злотенко Б.М. – д.т.н., проф., *zlotenko.bm@knutd.edu.ua*
Київський національний університет технологій та дизайну

Метою роботи є організація безпеки мережевої інфраструктури підприємства в сучасних умовах.

З постійно зростаючим використанням комп'ютерних систем, хмарних інтернет-додатків для обміну даними та зв'язку, потреба в забезпеченні мережевої безпеки є важливою для всіх типів організацій, починаючи від підприємств, академічних або державних установ, до географічно розкиданих кінцевих користувачів з різними ролями та профілями [1]. Цей різноманітний діапазон створює багато нових проблем для стандартних традиційних підходів до забезпечення безпеки мережевої інфраструктури.

Політика безпеки є одним із найважливіших засобів контролю в будь-якій організації. Ці засоби контролю включають безпеку мережі та описують конкретну технологію, апаратне забезпечення або програмне забезпечення, яке буде використовуватися. Безпека мережі базується на прийнятих нормативних актах і внутрішніх політиках підприємства та впроваджується й контролюється його мережевими адміністраторами як запобігання несанкціонованому доступу та неправильному використанню даних. [2, 3].

Кожне підприємство зобов'язане встановлювати та дотримуватися організаційних політик, процедур та рекомендацій щодо створення інструкцій з правилами встановлення комп'ютерних систем та додатків; створення посібника з побудови локальної мережі; створення посадових інструкцій працівників і регулювання їх роботи з комп'ютерними системами та електронними документами.

Безпека мережі реалізується за допомогою набору завдань і інструментів, які використовуються підприємством для захисту від несанкціонованого доступу до комп'ютерних мереж і пов'язаних з ними пристроїв та програм. Різні рівні безпеки застосовуються для забезпечення безпеки мережі [4], тому зловмисник повинен скомпрометувати два або більше рівня для отримання доступу до критичних для підприємства активів.

У мережі повинні бути реалізовані стратегії безпеки мережі, моніторингу та відновлення політики безпеки. Безпека означає, що всі системи та мережі повинні бути налаштовані якомога коректніше, дотримуючись останніх рекомендацій виробника та передових практик. Моніторинг означає, що потрібно постійно ідентифікувати зміни в конфігурації, мережевий трафік, нетиповий для мережі або систем, які в ній працюють. Відновлення означає, щоу випадку, коли виявлено проблему, пристрої та системи необхідно відновити до останньої версії безпечний стан якомога швидше.

Мережа потребує значної оборонної стратегії для захисту окремих компонентів та інформації, яку вони містять. Має бути реалізовано декілька рівнів захисту від зовнішніх загроз для периметру мережі, а також для моніторингу та обмеження вхідного і вихідного трафіку. Необхідно налаштувати та встановити пристрої безпеки по периметру мережі відповідно до найкращих практик безпеки: впровадити кілька рівнів брандмауерів нового покоління по всій мережі, щоб обмежити вхідний трафік, обмежити вихідний трафік і перевірити всю внутрішню активність між різними частинами мережі; впровадити рішення моніторингу мережі для реєстрації та відстеження вхідних і вихідних повідомлень трафіку; розгорнути кілька виділених віддалених серверів, щоб увімкнути кореляцію активності серед пристроїв; впровадити резервні пристрої в основних частинах мережі для забезпечення доступності, для збільшення пропускної здатності мережі та зменшення затримки.

Подібні системи в мережі мають бути логічно згруповані разом для захисту від вторгнення. Правильна сегментація мережі зменшує здатність зловмисників досягати й використовувати різні системи [5], [6]. Крім того, обмеження доступу між різними типами систем забезпечує легше керування та контроль, якщо вони логічно згруповані разом.

Для забезпечення зашифрованого доступу до каналу зв'язку через мережу між двома кінцевими точками може бути встановлений VPN-тунель. Його слід використовувати лише при дотриманні конфіденційності і цілісності трафіку, оскільки неможливо підтримувати іншими методами. VPN шлюзи зазвичай доступні з Інтернету та схильні до мережевого сканування.

Таким чином, правильне адміністратори відіграє вирішальну роль у захисті мереж від ворожих загроз. Дотримання заходів кібербезпеки допоможе забезпечити зниження ризику компрометації та гарантувати більшу безпечність та кращу захищеність мережі підприємства.

Література

1. Saikeerthana R, Umamakeswari A. Secure data storage and data retrieval in cloud storage using cipher policy attribute based encryption. Indian Journal of Science and Technology. 2015 May; 8(S9).– P. 1-8.

2. Tipton H. F., Krause M., Information Security Management Handbook, Fifth Edition, CRC Press, Dec. 30, 2003 - Computers - 2036 p.

3. What Is Network Security?
https://www.cisco.com/c/en/us/products/security/what-is-networksecurity.
html#~types-of-network-security, accessed January 2020.

4. Rexha B., Qerimi E., Neziri V., Dervishi R. Using eID Pseudonymity and Anonymity for Strengthening User Freedom in Internet, CEEE|Gov Days 2015, National University of Public Service, Budapest, Hungary, Vol. 1, P. 1-9.

5. Cybersecurity and Infrastructure Security Agency (2022), Layering Network Security Through Segmentation. Available at:
https://www.cisa.gov/sites/default/files/publications/layering-networksecurity segmentation_infographic_508_0.pdf

6. National Security Agency (2019), Segment Networks and Deploy Application-aware Defenses. Available at: https://www.nsa.gov/cybersecurity-guidance