УДК 004.056.53

ОСОБЛИВОСТІ ПОБУДОВИ ЗАХИЩЕНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

Кленик О., Ткачук Р.
Львівський державний університет безпеки життєдіяльності, м .Львів

В роботі прорведено дослідження із організації захисту корпоративної мережі. Описані особливості вистановлення контролю периметру корпоративної мережі, організація безпеки всередині самої мережі. А також розглянуто заходи із підвищення захищеності систем в аспекті зменшення поверхні можливої атаки на мережу.
Ключові слова: *локальна мережа, безпека, захист, контроль.*

The research on the organization of corporate network protection is carried out in the work. Features of establishment of control of perimeter of a corporate network, the organization of safety within the network are described. Also, measures to increase the security of systems in terms of reducing the surface of a possible attack on the network are considered.
Keywords: *local network, security, protection, control.*

Зі збільшенням обсягу даних, які використовуються користувачами інформаційної системи, збільшуються труднощі у веденні успішного бізнесу. Одним з найважливіших завдань для успішного функціонування інформаційної системи компанії є забезпечення збереження даних у мережі.

Для того, щоб зберегти конфіденційність даних всередині компанії, необхідно налаштувати систему інформаційної безпеки. Однак при її побудові потрібно зберегти принципи конфіденційності, цілісності та доступності. Але без виявлення та оцінки ризиків налагодити систему інформаційної безпеки неможливо. Хоча міжнародний стандарт ISO 27000 не визначає, який метод слід використовувати для оцінки ризиків, це завдання зазвичай покладається на керівників або відповідальних за створення системи захисту інформації в компанії.

Контроль периметру корпоративної мережі

Для того, щоб створити безпечну мережу, контроль спочатку вводиться на периметр мережі компанії. Для контролю трафіку використовуються мережеві екрани з функціями керування на рівні програми та системи контролю вторгнень (ips) – next generation firewal (NGFW). Публічні сервіси встановлюють в окремих нейтральних зонах і налаштовують правила доступу для контролю потоків даних і відмови від використання загальних сутностей, таких як «any», «all» [1].

Також для захисту периметра необхідно використовувати проксі-сервер для контролю доступу в Інтернет користувачів. Також необхідно

заблокувати доступ до ресурсів із забороненою тематикою, поганою репутацією, високим ризиком та фішинговими ресурсами. Антивірусне сканування та фільтрація завантаження вмісту є обов'язковими. Зокрема, потрібно заблокувати завантаження виконуваних файлів для звичайних користувачів. Також необхідно налаштувати повне сканування SSL для виявлення загроз у зашифрованому трафіку. Відповідно, необхідно організувати заборону на використання безумовних білих списків для доступу до зовнішніх ресурсів та організувати білі списки внутрішніх систем в обхід правил тематичного огляду [3, 4].

Зокрема, щоб створити безпечний периметр, потрібно використовувати електронний шлюз для захисту корпоративної електронної пошти від спаму та зовнішніх загроз. Передача інформації між підрозділами компанії та з віддаленим доступом користувачів через Інтернет-канали має відбуватися тільки через VPN з відповідним рівнем шифрування (aes-256 і вище) та з обов'язковим моніторингом і фіксацією вжитих заходів. Все це стосується як зовнішніх партнерів, так і підрядників компанії.

Безпека локальної мережі

Однак недостатньо лише створити захищений периметр мережі необхідно організувати належний рівень безпеки в самій мережі.

Спочатку потрібно сегментувати локальну мережу за функціональним призначенням, тобто розділити сервіси на відповідні сегменти сервера. Крім того, необхідно заборонити створення сегментів у великій кількості систем, оскільки технологія VLAN дозволяє створити сегмент із 4096 пристроями. Для особливо критичних систем і сервісів необхідно мікросегментувати мережу, в ідеалі за принципом один сегмент - одна система.

Також потрібно ізолювати порти на комутаторах доступу користувачів, щоб уникнути прямої взаємодії між системами користувача. Технології захисту від атак, такі як ARP-спуфінг і DHCP-серверів, також повинні бути налаштовані, щоб запобігти перехопленню трафіку даних [3].

Також необхідно заблокувати пряму мережеву взаємодію між Інтернет-сервісами та корпоративною мережею. Зв'язок між сегментами має відбуватися тільки через проксі-сервери, які розташовані в нейтральних зонах на вузлі мереж. Крім того, трафік між нейтральною зоною та ресурсами Інтернету, а також між нейтральною зоною та корпоративною мережею повинен контролюватися брандмауерами.

Захищеність корпоративних систем

Наступним кроком буде підвищення безпеки систем, що експлуатуються в організації (мережевих пристроїв, серверних і користувацьких систем) з метою зменшення можливої зони атаки на мережу [4].

Необхідно видалити та деактивувати зайві компоненти та служби, які не використовуються або не потрібні в робочому процесі. Також слід уни-

кати використання застарілих протоколів, таких як NTML, SMBv1 тощо. Слід вжити механізмів та заходів для протидії передачі паролів з пам'яті та системних процесів.

Також потрібно заборонити створення локальних облікових записів або змінювати їхні паролі, оскільки інформація про обліковий запис і пароль доступна всім користувачам мережі. Регулярні оновлення системного та прикладного програмного забезпечення також повинні дозволяти блокувати механізм автоматичного виявлення проксі-серверів WPAD.

Необхідно постійно перевіряти, що на сервері та системі організації встановлено новітнє антивірусне програмне забезпечення, і регулярно оновлювати його. Крім того, організувати наявність в системах організації встановленого рішення Host IPS з увімкненим функціоналом [2]:

– брандмауер з налаштованими мінімальними дозволами, необхідними для роботи;

– захист сигнатур від атак як на рівні мережі, так і всередині самої системи;

– блокування невідомих процесів в робочій і системній пам'яті;

– поведінковий аналіз дій програмних процесів і блокування у разі підозрілої діяльності;

– блокування підлеглих процесів, які створюють документи Office.

І нарешті, потрібне рішення для контролю підключення периферійних пристроїв і знімних носіїв до робочих станцій організації. Крім того, слід налаштувати правила для підключення до корпоративної мережі лише перевірених корпоративних носіїв.

Література

1. Методи захисту мереж [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://studopedia.su/6_4733_metodi-zashchiti-setey.html.

2. Росляков О. О. Віртуальні приватні мережі. Основи побудови та застосування / О. О. Росляков, С. В. Попов. – Київ: Еко-трендз, 2006. – 301 с. Snader J. J. VPNs illustrated: Tunnels, VPN's and IPsec / John Junior Snader., 2006. – 445 с.

3. Захист мережі: комплексний підхід [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://goo.su/16VM.

4. Концепції захисту IT-інфраструктури від сучасних загроз [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://netwave.ua/ru/kontseptsy-ya-zashhy-ty-y-t-y-nfrastruktury-ot-sovremenny-h-ugroz.