МЕРЕЖНА БЕЗПЕКА, СИСТЕМИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ АТАКАМ, ВІДМОВОСТІЙКІСТЬ МЕРЕЖ

Тертичний В.О.
Науковий керівник – док.т.н. Шостко І.С.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-55-92)

In recent years, the number of deliberate interventions (hacker or cyber attacks) in the work of information systems of all state and commercial structures has sharply increased in Ukraine. In almost all cases, after the implementation of hacker attacks, the work of enterprises is blocked from several hours to several days, which leads to significant financial losses. The article describes the main points of network security in general, It also talks about network resiliency. A set of measures to protect the network was also proposed.

Мережною безпекою називаються дії, спрямовані на захист працездатності і цілісності мережі і даних. Основне завдання мережної безпеки – це збалансований захист конфіденційності, цілісності і доступності даних, з урахуванням доцільності застосування і без будь-якої шкоди продуктивності організації. До основних методів мережної безпеки можна віднести такі методи як:

1. авторизація користувачів;
2. антивірусне ПЗ;
3. безпека електронної пошти;
4. сегментування мережі;
5. використання систем виявлення та протидії атакам;
6. використання брандмауеру;
7. відмовостійкість мережі.

Для того щоб захистити мережу необхідно в першу чергу захистити периметр мережі, тобто її зовнішній кордон. Захист периметра вважається обов'язковим елементом системи забезпечення інформаційної безпеки корпоративної мережі і включає в себе шлюзи безпеки, засоби міжмережевого екранування, організацію віртуальних приватних мереж (VPN), системи виявлення та запобігання вторгнень (IDS / IPS).

Замість того щоб боротися з наслідками інцидентів безпеки, а виявити їх відразу необхідно використовувати системи виявлення вторгнень, які призначені для визначення фактів несанкціонованого доступу до комп'ютерної системи чи мережі або несанкціонованого управління ними в основному через Інтернет.

Зазвичай архітектура системи виявлення вторгнень включає такі компоненти як: сенсорну систему, призначену для збору подій; підсистему

аналізу, призначену для виявлення атак; сховище в якому зберігаються результати аналізу; консоль управління. Системи виявлення вторгнень можна поділити на дві основні категорії: пасивні (IDS) і активні (IPS).

Різниця між ними ж полягає в тому, що в активній системі виявлення вторгнень, системою відразу ж приймаються відповідні дії на порушення такі як скидання з'єднання тощо.

Використання ноутбуків і смартфонів дозволяє співробітникам працювати, перебуваючи поза офісом. Їм необхідно забезпечити захищений віддалений доступ до корпоративних додатків, не знижуючи при цьому рівня безпеки. Тому систему мережної безпеки необхідно доповнити системами управління мобільними пристроями, додатками і даними.

Найчастіше вибір падає на так звані брандмауери наступного покоління (NGFW) — системи корпоративного класу, що забезпечують багаторівневий захист на базі одного пристрою. Таким чином, система захисту периметра розширюється і доповнюється іншими рішеннями, але ні в якому разі не скасовується .

Якщо говорити про відмовостійкість мережі то рівень надійності мережі залежить від рівня і типу відмовостійких рішень, застосованих в мережі. Відмовостійкість мережі визначається двома факторами: рівень надмірності мережної інфраструктури; час відновлення мережі, тобто час, необхідний для перемикання потоків даних на працездатні частини мережі в разі відмови її частини. Для підвищення відмовостійкості необхідно приймати такі міркування при проектуванні мережі: архітектура мережевого обладнання; дублювання з'єднань; рознесення каналів зв'язку.

У висновку роботи хочеться додати, що для забезпечення високого рівня корпоративної безпеки потрібно використовувати цілий комплекс заходів захисту. Перш за все потрібно побудувати зовнішній периметр мережі з використанням технологій VPN, систем виявлення та запобігання вторгненням, а також міжмережевими екранами. Також необхідно організувати захищені з'єднання для віддалених користувачів. Адже боротьба з новими атаками вимагає рішень по забезпеченню мережної безпеки і розробки мережної стратегії безпеки, що відповідає вимогам надійності, вартості та питань інтеграції з іншими IT системами. Вироблені рішення повинні бути надійними, забезпечувати захист від атак на рівні додатків і дозволяти ідентифікувати трафік.

Перелік посилань

1. Що таке мережева безпека? [Електронний ресурс]. – Режим доступу до ресурсу: https://www.cisco.com/c/ru_ru/products/security/what-is-network-security.html (дата звернення 15.02.2020)

2. Мережева безпека. Замість введення? [Електронний ресурс]. – Режим доступу до ресурсу: https://habr.com/ru/company/hpe/blog/261913/ (дата звернення 15.02.2020)