Добри практики в мрежовата сигурност

MikroTik Net Camp 2017

Трявна

Петър Димитров

За мен:

- Име: Петър Димитров
- Опит в областта на компютърните мрежи: от 2002 г.
- Опит с MikroTik: от 2005 г.
- MikroTik Trainer: от 2013 г.
- Предлагани MikroTik обучения:

MTCNA, MTCWE, MTCRE, MTCTCE, MTCUME, MTCIPv6E, MTCINE

Проблем ли е сигурността?

- Днес сме изцяло зависими от компютърните мрежи.
- Бизнес, индустрия, комунални услуги и стратегически обекти обвързват процесите си с компютърните мрежи и Интернет.

Проблем ли е сигурността?

- В свят, където не само разглеждането на уеб сайтове зависи от мрежите, но чрез тях се управляват от осветлението и отоплението в домовете ни, през финанси и медицински услуги, всички бизнес процеси и комуникации, до потенциално опасните за живота ни управление на автомобили, самолети, заводи и даже военни действия, трябва да се обърне особено голямо внимание на мрежовата сигурност.

Технологични решения

- Технологиите сами по себе си не могат да решат проблема, те са само инструмент, управляван от нас.
- Хората, създаващи технологиите и управляващи мрежите не са съвършени, човешките грешки създават предпоставки за пробив в сигурността.
- Целта на тази презентация е да даде насоки за подобряване на сигурността с конкретни стъки при конфигуриране на MikroTik RouterOS.

Общи "животоспасяващи" практики

- Преди да се концентрираме върху "техническата" част, нека обърнем внимание на някои важни препоръки:
  - Поддържайте мрежови диаграми и списък с устройства, както и кой отговаря за тях.
  - Не използвайте един потребител за работа от всички колеги и не използвайте потребителите по подразбиране. Централизирано управление на потребителите дава предимства.

Общи "животоспасяващи" практики

- SNMP достъпа до утройствата (макар и само за четене) е полезен за Вас, но при неправилна конфигурация може да бъде полезен и за злонамерени хакери.
- Наблюдавайте мрежата чрез подходяща система (NMS), така ще бъдете информирани своевременно за състоянието ѝ.
- Използвайте централизирана система за съхранение на журнали (log-ове), по възможност с опция за анализ и следене за отклонения от нормалното и предупреждения.
- Периодично сканирайте за уязвимости (vulnerability scans) както отвън, така и отвътре и сравнявайте резултата с предните сканирания.

OSI модел

Layer 1

- Физическия достъп до мрежата крие рискове от:
  - Компрометиране на конфиденциалността и/или интегритета на пренасяните данни.
  - Инсталиране на чуждо устройство в мрежата.
  - Достъпване на информация, съхранявана на мрежовите устройства.

Преносна среда

- Поради естеството на преносната среда, достъпа до безжично предавана информация е значително по-лесен от достъпа до информация, предавана по кабел (меден или оптичен). В безжични мрежи можете да използвате:
  - WPA2PSK с AES криптиране.
  - Сигурност по MAC адрес (access list и connect list).
  - Между две MikroTik устройства - Management Frame Protection.
- Можете да комбинирате с допълнителна защита на пренасяните данни.

Чуждо устройство в мрежата

- Обикновено повечето от мерките за сигурност са в посока отвън навътре. Чуждо устройство във вътрешната мрежа може да изпраща данни или да се свърже отвътре навън и да осигури достъп през създадената връзка до вътрешни ресурси.
- Можете да затрудните такъв сценарий чрез:
  - Забраняване на всички неизползвани портове на мрежови устройства (рутери и суичове).
  - Осигуряване на достъп до Интернет само на описаните ваши устройства.

Физически достъп до мрежови устройства

- Крие опасност от reset на устройството, с последващ достъп до съхранените в него файлове.
- Крие опасност устройството да бъде накарано да boot-не по мрежата чужда OS, с помощта на която да бъдат достъпени файлове и/или конфигурация, включително системни, включително да се открадне акаунт за достъп.

Физически достъп до мрежови устройства

- Можете да:
  - не съхранявате export и некриприрани backup файлове на устройството.
  - използвате Protected Routerboot.

Layer 2

- ARP poisoning/spoofing - чрез изпращане на фалшиви ARP съобщения недобронамерен хост може да предизвика свързване на определен IP адрес с неговия MAC адрес в таблиците на другите хостове в локалната мрежа, водещо до насочване на трафик към него (най-често с цел Man-In-The-Middle атака).
- Неоторизирани DHCP сървъри.
- Достъп до мрежови устройства (рутери и суичове) на Layer 2.

ARP poisoning/spoofing

- Към момента няма механизъм за динамично решение на проблема. Други производители имат решения, базирани на сравнение на ARP съобщенията с таблица, изградена на база обменените DHCP съобщения и блокиране на порт при несъответствие. Решенията имат смисъл само на суичовете, към които се свързват хостовете.
- Решение на проблема е статично попълване на ARP таблиците.
- На рутера може да се конфигурира режим на работа на ARP протокола "reply-only" на съответния интерфейс (може да се комбинира с опцията "add-arp" на DHCP сървъра).

Неоторизирани DHCP сървъри

- В резултат от появяване на чужд DHCP сървър в мрежата, хостове могат да получат некоректни настройки.
- В най-добрия случай тези хостове няма да имат достъп до мрежата, а в най-лошия - може това да е част от Man-In-The-Middle атака.

Неоторизирани DHCP сървъри

- Решението на проблема е използване на "умни" суичове, повечето CRS имат необходимата функционалност, за да разрешите DHCP сървъри само зад портовете, където се намират вашите сървъри.
- При невъзможност за такава имплементация, в RouterOS има инструмент "/ip dhcp-server alert", който може да е от полза за ранно установяване на проблем, а DHCP сървъра може да бъде "authoritative", което да помогне за по-бързо възстановяване след инцидент.

Layer 2 достъп до устройства

- RouterOS може да бъде достъпен на Layer 2:
  - по MAC Telnet
  - по MAC Winbox
  - през RoMON
- Забранявайте тези видове достъпи от публични или несигурни сегменти.

Neighbor Discovery

- MikroTik Neighbor Discovery Protocol (MNDP) позволява на вашия рутер да открива и да бъде откриван от други устройства, поддържащи MNDP, CDP (Cisco Discovery Protocol) и Link Layer Discovery Protocol (LLDP).
- Изпращането на информация за устройство, версия, адреси и др. в несигурни сегменти крие рискове.
- Можете да забраните Neighbor Discovery на публичните интерфейси.

Layer 3 - динамична маршрутизация

- Най-често използваните динамични маршрутизиращи протоколи са OSPF и BGP.
- При неправилна конфигурация съществуват начини за атакуване на мрежата чрез тези протоколи.
- Ще разгледаме някои идеи, които да намалят този риск:

OSPF

- Не използвайте OSPF между вас и чужда AS. Забранете протокол 89 (OSPF) отвън още на вашите Border рутери.
- Дистрибутирайте потребителските мрежи като външни, не ги вкарвайте в OSPF процеса. Ако това е наложително - конфигурирайте интерфейсите като пасивни.
- Използвайте MD5 автентикация, това ще забави атакуващия.
- Използвайте правилните видове области.

BGP

- Използвайте MD5 автентикация, това ще забави атакуващия.
- Използвайте loopback за BGP peering.
- Фиксирайте TTL.
- Криптирайте BGP сесията :)

BGP и Routing Filters

- Обявявайте само вашите префикси.
- Не приемайте отвън:
  - собствените си префикси
  - BOGONS
  - маршрут по подразбиране
  - префикси с prefix lenght > 24

Layer 3, Layer 4

- Едно от най-съществените условия да постигнете желаното ниво на сигурност е да планирате и реализирате подходяща концепция за защитна стена (firewall).
- Добър подход е разрешаване само на:
  - необходимите услуги
  - от сигурни източници
  - с допустимо натоварване

Задължително ли трябва да има защитна стена (firewall)?

- Краткия отговор е ДА! Ако сигурността е от значение, това е начина да я постигнете.
- Не се подвеждайте:
  - Смяната на стандартните портове на услугите не дава сигурност.
  - NAT не е средство за сигурност.
  - Ограничаването на достъпността на услугите в /ip services не скрива отворения порт.

Услуги в /ip services

- Спрете всички услуги, които не използвате.
- Достъпвайте рутера си само чрез защитени услуги - secure winbox, https, api-ssl.
- Никога не правете telnet през Интернет.

Достъп до ресурси/услуги

- Ако трябва да осигурите отдалечен достъп до ресурси и услуги, които не са публични:
  - Опитайте да ограничите от къде могат да се достъпват ресурсите.
  - Използвайте вариант на port knock.
  - Най-добрия начин за защита и контрол е ресурсите да се достъпват само чрез VPN.

По-горни слоеве

Layer 5, Layer 6, Layer 7

- Осигурявайки мрежови услуги, обикновено контрола върху по-горните слоеве не зависи от мрежовите администратори.
- В някои случаи можем да се възползваме от разпознаване по Layer7 протокол, но не трябва да забравяме:
  - RouterOS събира първите 10 пакета или 2KB от връзката и търси модела в тях.
  - Това е много ресурсоемък процес.

Layer 8 - Money, Layer 9 - Politics :)

- Повишаването на сигурността не трябва да бъде самоцел - винаги трябва да се търси баланс между инвестициите в сигурност и критичността на защитаваните ресурси.
- Не е адекватно да създадете и поддържате частна армия за охрана на един хамбургер!

Layer 8 - Money, Layer 9 - Politics :)

- Закупуването на техника не е достатъчно, хората трябва да бъдат обучавани.
- Успешното прилагане на политики изисква налагане на промяна и правила отгоре и убеждаване на потребителите, че сигурността е нещо важно и то зависи от тях.

Какво друго?

- Какво следва?
- Време е да направим базова конфигурация на рутер!

Благодаря за вниманието!