Основные виды СЗИ

Teach Me Skills

Вопросы по предыдущим темам или ДЗ

Mini-quize по новой теме:

1. **Как работает система обнаружения вторжений?**
2. **Может ли помочь провайдер с защитой от DDOS?**
3. **К какой категории средств ИБ относится программа Suricata?**
4. **Что такое Windows Defender?**
5. **В какое место сетевой схемы устанавливают IDS?**

Teach Me Skills

План занятия

1. Защита почтовых серверов, антиспам системы
2. Anti DDoS, защита от Брутфорсов
3. IDS, IPS
4. Использование WIndows Defender (Windows Security)

Основные виды СЗИ

DoS-атаки:

- начинаются неожиданно (не нужна разведка и подготовка);
- развиваются очень быстро;
- способны полностью заблокировать работу сервера;
- почти невозможно определить злоумышленника.

DoS-атаки: проблемы построения защиты

Чаще всего трафик является законным, как это определено протоколом.

Используется огромный трафик, в том числе через ботнетов. Этот же трафик и должны обрабатывать средства защиты.

Атаки на уровне приложений используют определенные приложения или службы в целевой системе. Этот список постоянно меняется и его нужно отслеживать.

Основные виды СЗИ

Решение защиты от DoS-атаки: устройства с отслеживанием

Плюсы:
- чаще всё реализуется на уровне межсетевого экрана;
- на основе анализа пакета создается таблица состояний соединения, что позволяет отбрасывать неактивные или “мусорные” соединения.

Минусы:
- данный тип устройств защищает не от всех типов DoS-атак;
- для каждого соединения создается своя таблица состояний, поэтому нагрузка многократно возрастает на само устройство защиты.

Решение защиты от DoS-атаки: фильтрация маршрутов

Если удалось определить сетевые маршруты, по которым развивается атака, то возможно создание “черных дыр”.

Сетевая черная дыра (black hole) - это “места”, куда будет перенаправляется и сбрасываться трафик, по аналогии с устройством /dev/null в ОС Linux.

Черная дыра может полностью “поглотить” весь трафик атаки, но для этого нужно точно указать IP-адреса назначения или источника.

Основные виды СЗИ

Решение защиты от DoS-атаки: распределение сетевых ресурсов

Географическое распределение (Geographic Dispersion, Global Resources Anycast) - распределение сетевых мощностей на отдельные узлы.

Anycast - это метод маршрутизации, который позволяет направлять трафик от одного источника к различным сетевым узлам (представляющим один и тот же IP-адрес).

Решение защиты от DoS-атаки: ограничение соединений и тайм-аутов

Ограничение соединений и тайм-аутов чаще всего используются во внутренних сетях, где время передачи мало.

Такие ограничения направлены на то, чтобы гарантировать, что DDoS-атаки не запускаются и не распространяются изнутри сети намеренно или непреднамеренно.

Основные виды СЗИ

Решение защиты от DoS-атаки: списки контроля доступа

Списки контроля доступа (Access Control Lists, ACL) используются для защиты сетей от нежелательного трафика с помощью фильтрации по набору заданных правил.

Например, ACL может запретить или разрешить HTTP-трафик только на определенные сайты, используя IP-адрес или группу IP-адресов.

Основные виды СЗИ

Решение защиты от DoS-атаки: Scrubbing and Diversion

Traffic Scrubbing and Diversion (очистка и изменение направления трафика) - отдельная услуга по защите от DDoS-атак.

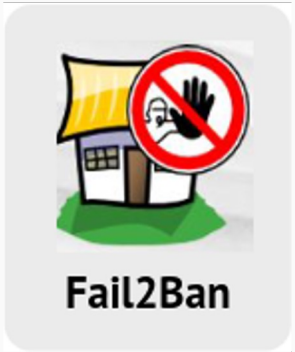
Чаще всего трафик организации или внешний трафик перенаправляется во внутреннюю сеть поставщика решения, фильтруется и уже “в чистом виде” передается на вход клиента.
В основном, такую услугу предоставляют провайдеры, т.к. у них уже есть готовая инфраструктура и запас мощностей.

Основные виды СЗИ

Fail2Ban: введение

Fail2Ban - одна из узкоспециализированных систем обнаружения вторжений
(СОВ, Intrusion Prevention Software, IPS).

Fail2Ban сканирует лог-файлы, находит в них странное сетевое поведение (например, ошибки набора пароля) и блокирует подозрительные адреса IP-адреса на заданное время.

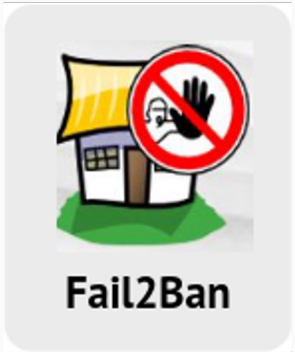


Fail2Ban: установка

ubuntu@ubuntu:~$ sudo apt install fail2ban

Файл с настройками (необходимо скопировать в jail.local):
/etc/fail2ban/jail.conf

Файл с фильтрами:
/etc/fail2ban/filter.d



Основные виды СЗИ

Hydra

Hydra (THC-Hydra) - инструмент для подбора подбора паролей к сервисам, защищённым аутентификацией. Умеет работать с большим количеством протоколов (SSH, FTP и другие).

Пример Атаки на SSH

kali@kali:~$ hydra -L users.txt -P pass.txt 192.168.0.5 ssh

```
kali@kali:~$ hydra -L users.txt -P pass.txt 192.168.0.5 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting a
[WARNING] Many SSH configurations limit the number of paralle
[DATA] max 16 tasks per 1 server, overall 16 tasks, 56 login
[DATA] attacking ssh://192.168.0.5:22/
[22][ssh] host: 192.168.0.5   login: user   password: user
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished a
```

fail2ban: повторная атака

Повторим предыдущий пример после установки fail2ban:

kali@kali:~$ hydra -L users.txt -P pass.txt 192.168.0.1 ssh

Рано или поздно (при включенном fail2ban) получим:
[ERROR] could not connect to ssh://192.168.0.1:22 - Connection refused

Проверим лог-файл:
ubuntu@ubuntu:~$ tail /var/log/auth.log
Oct 22 16:41:37 ubuntu sshd[3520]: Failed password for invalid user postgres from 192.168.0.2 port 40730 ssh2

ubuntu@ubuntu:~$ cat /var/log/fail2ban.log
2020-10-22 16:1:37 NOTICE [sshd] Ban 192.168.0.2

Основные виды СЗИ

Система Обнаружения Вторжений

Система Обнаружения Вторжений (Intrusion Detection System, IDS) - программное или аппаратное решение, определяющее вредоносную активности в системе или сетевом трафике.

Система Предотвращения Вторжений (Intrusion Prevention Systems, IPS) - программное или аппаратное решение, предотвращающее вредоносную активности в системе или сетевом трафике.
В документах и IDS, и IPS пишут как “СОВ”. Иногда, IPS обозначают как “активная СОВ”.

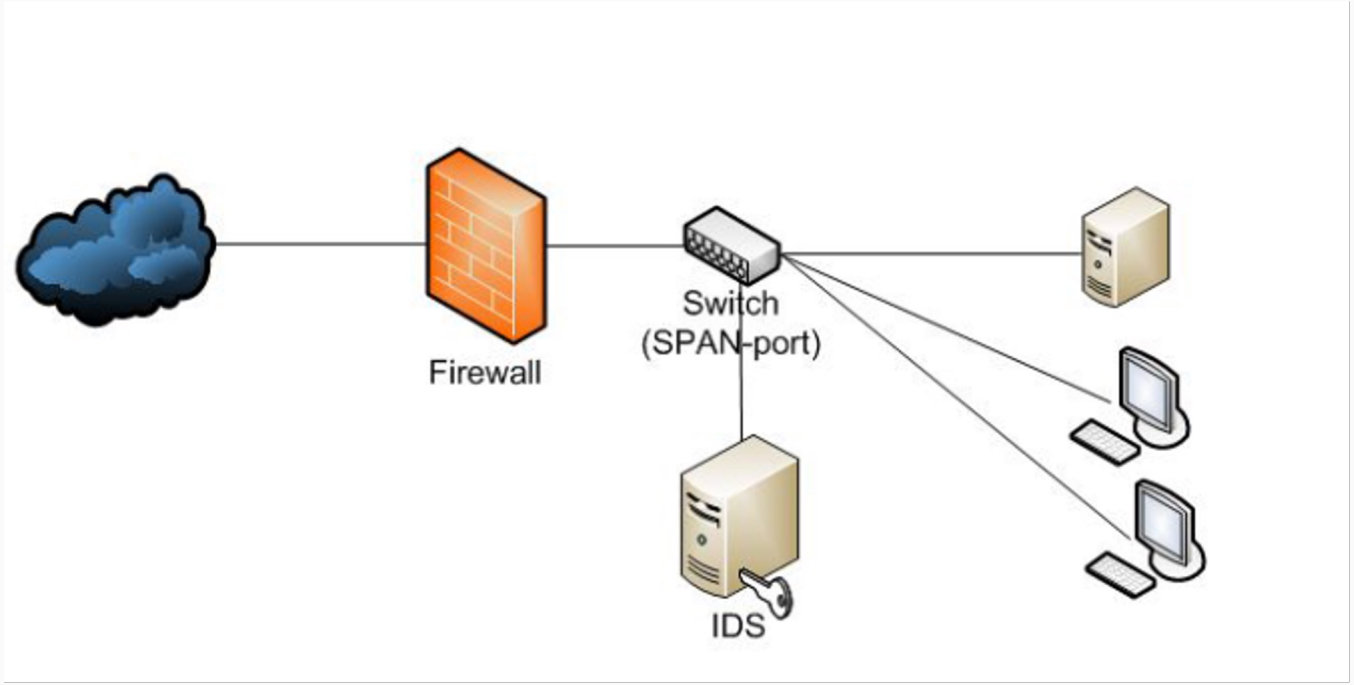
Основные виды СЗИ

Система Обнаружения Вторжений - как работает

1. Захват сетевого трафика.
2. Сборка потоков (stream reassembly) – выделяются TCP, UDP и т.д.
3. Разбор протоколов (protocol parsing) – выделяются высокоуровневые протоколы, нормализуются данные (data normalization: декодирование, распаковка и т.д.).
4. Применение сигнатур (signatures check).
5. Действия (action) – происходит оповещение пользователя, блокирование трафика и т.д.

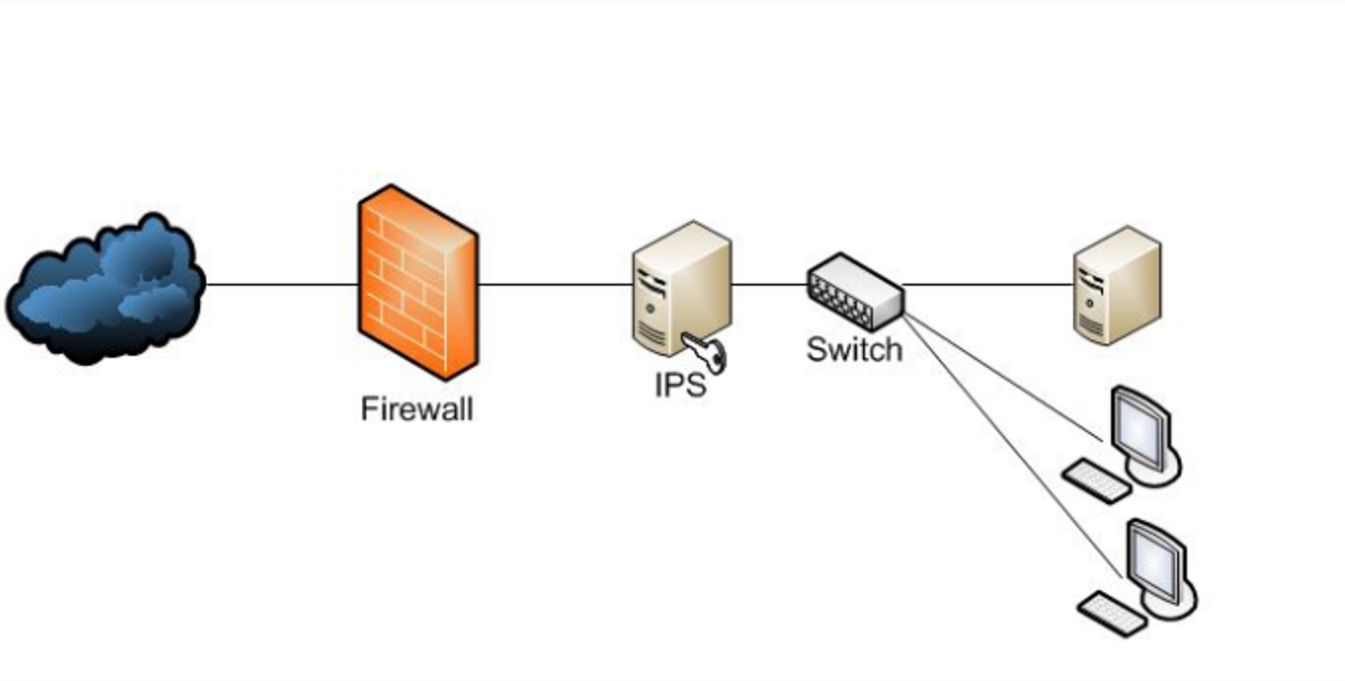
Основные виды СЗИ

Система Обнаружения Вторжений (IDS)



Основные виды СЗИ

Система Обнаружения Вторжений (IPS)



Основные виды СЗИ

Система Обнаружения Вторжений

По подключению:
- Сетевая СОВ (Network-based IDS, NIDS)
- Локальная СОВ (Host-based IDS, HIDS)

По методу обнаружения аномалий:
- Сигнатурный поиск (Signature-based detection)
- Статистическое определение аномалий (Statistical anomaly-based detection)

Система Обнаружения Вторжений - проблемы

Наличие ложно-позитивных срабатываний.

- Необходимо постоянное обновление правил.
- Существует временной лаг между появлением уязвимостей и созданием правил для их обнаружения.
- Невозможна обработка зашифрованного трафика.
- Почти невозможно определить уязвимости, вызванные неправильной настройкой (слабая аутентификации и т.д.).

Основные виды СЗИ

Suricata: введение

Suricata - сетевая IDS с открытым исходным кодом, разрабатываемая Open Security Foundation (OISF).
Сайт: suricata
Исходный код: github.com/OISF/suricata

Основные виды СЗИ

Suricata: Преимущества

многопоточность из коробки;
- возможность анализа файлов pcap;
- поддержка GPU (Cuda, OpenCL);
- поддержка развитые средства для проверки HTTP, IPv6;
- изначальная поддержка режима IPS;
- поддержка правил snort;
- вывод Unified2;
- автоматический анализ протоколов (может определить протокол
запущенный на нестандартных портах)

Основные виды СЗИ

Suricata: Установка

```
user@user:~$ sudo apt install software-properties-common
user@user:~$ sudo add-apt-repository ppa:oisf/suricata-stable
user@user:~$ sudo apt update
user@user:~$ sudo apt install suricata
user@user:~$ sudo suricata-update

Проверка установки:

user@user:~$ sudo systemctl status suricata
```

Основные виды СЗИ

Suricata: Настройка

```
user@user:~$ sudo nano /etc/suricata/suricata.yaml

И меняем значение параметра EXTERNAL_NET на "any"

user@user:~$ sudo systemctl restart suricata

Лог-файлы:

user@user:~$ sudo tail /var/log/suricata/suricata.log

user@user:~$ sudo tail /var/log/suricata/stats.log
```

Основные виды СЗИ

Suricata: Запуск

ubuntu@ubuntu:~$ sudo suricata -c /etc/suricata/suricata.yaml -i enp0s3

где параметр “i” указывает прослушиваемый интерфейс

откроем лог-файл, в котором будут отображаться предупреждения:
ubuntu@ubuntu:~$ sudo tail -f /var/log/suricata/fast.log

```
10/24/2020-21:58:26.979157  [**] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [**] [Classification: Potentially Bad Traffic] [Priority
: 2] {TCP} 192.168.0.1:33651 -> 192.168.0.3:3306
10/24/2020-21:58:26.979158  [**] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [**] [Classification: Potentially Bad Traffic] [Priority
: 2] {TCP} 192.168.0.1:33651 -> 192.168.0.3:3306
10/24/2020-21:58:26.981754  [**] [1:2010939:3] ET SCAN Suspicious inbound to PostgreSQL port 5432 [**] [Classification: Potentially Bad Traffic] [Pri
ority: 2] {TCP} 192.168.0.1:33651 -> 192.168.0.3:5432
10/24/2020-21:58:26.981754  [**] [1:2010939:3] ET SCAN Suspicious inbound to PostgreSQL port 5432 [**] [Classification: Potentially Bad Traffic] [Pri
ority: 2] {TCP} 192.168.0.1:33651 -> 192.168.0.3:5432
10/24/2020-21:58:26.987262  [**] [1:2010936:3] ET SCAN Suspicious inbound to Oracle SQL port 1521 [**] [Classification: Potentially Bad Traffic] [Pri
ority: 2] {TCP} 192.168.0.1:33651 -> 192.168.0.3:1521
10/24/2020-21:58:26.987262  [**] [1:2010936:3] ET SCAN Suspicious inbound to Oracle SQL port 1521 [**] [Classification: Potentially Bad Traffic] [Pri
ority: 2] {TCP} 192.168.0.1:33651 -> 192.168.0.3:1521
10/24/2020-21:58:26.994955  [**] [1:2002911:6] ET SCAN Potential VNC Scan 5900-5920 [**] [Classification: Attempted Information Leak] [Priority: 2] {
```

Основные виды СЗИ

Suricata: Документация

- Инструкция пользователя
- Правила

Основные виды СЗИ

Suricata: Формат правил

- Действие (action) – что делать, если сигнатура совпала;
- Заголовок (header) – протокол, адрес, порт, направление;
- Параметры (options) – дополнительные данные правила.

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:”ET TROJAN
Likely Bot Nick in IRC (USA +..)”; flow:established,to_server;
flowbits:isset,is_proto_irc; content:”NICK “; pcre:”/NICK .*USA.*[0-9]{3,}/i”;
reference:url,doc.emergingthreats.net/2008124;
classtype:trojan-activity; sid:2008124; rev:2;)
```

Основные виды СЗИ

Suricata: Действия

- alert (предупреждение);
- pass (пропустить, не проверять дальше);
- drop (уничтожить пакет и показать предупреждение);
- reject / rejectsrc (послать RST / ошибку ICMP отправителю);
- rejectdst (послать RST / ошибку ICMP получателю);
- rejectboth (послать RST / ошибку ICMP отправителю и получателю).

Основные виды СЗИ

Suricata: Заголовок - протокол

Основные протоколы:
- tcp;
- udp;
- icmp;
- ip.

Дополнительные (если включены в suricata.yaml):
http, ftp, tls, smb, dns, dcerpc, ssh, smtp, imap, modbus, dnp3, enip, nfs, ikev2, krb5, ntp, dhcp, rfb, rdp, snmp, tftp, sip, http2.

Suricata: Направление трафика

Основные протоколы:
- tcp;
- udp;
- icmp;
- ip.

Дополнительные (если включены в suricata.yaml):
http, ftp, tls, smb, dns, dcerpc, ssh, smtp, imap, modbus, dnp3, enip, nfs, ikev2, krb5, ntp, dhcp, rfb, rdp, snmp, tftp, sip, http2.

Отправитель и получатель:
drop tcp $HOME_NET any -> $EXTERNAL_NET any
отправитель -> получатель
отправитель <> получатель (оба направления)
отправитель <- получатель отсутствует!

Suricata: Порты

Отправитель и получатель:
drop tcp $HOME_NET any -> $EXTERNAL_NET any
Операторы:
- : – диапазон портов;
- ! – отрицание или исключение;
- [..., ...] – группировка.

Более сложные примеры:
[80, 8080, 8888], [8000:9000, ![8080, 8100]]

Suricata: Параметры правила

/var/lib/suricata/rules - директория с правилами

drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:”ET TROJAN Likely Bot Nick in IRC (USA +..)”; flow:established,to_server; flowbits:isset,is_proto_irc; content:”NICK “; pcre:”/NICK .*USA.*[0-9]{3,}/i”; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124; rev:2;)

Параметры – это строки вида:
<ключевое слово>: <значение>;
<ключевое слово>;

Символы “ и ; являются зарезервированными и должны экранироваться в параметрах: \” и \;

Suricata: Параметры правила

Для Suricata существует ряд свободно распространяемых баз правил. Включить или отключить их можно при помощи утилиты suricata-update (устанавливается совместно с Suricata по умолчанию):

sudo suricata-update

Увидеть список доступных источников правил позволяет команда:
sudo suricata-update list-sources

Обновить список источников позволяет команда:
sudo suricata-update update-sources

Для включения доступного источника правил из списка необходимо выполнить две команды:
sudo suricata-update enable-source oisf/trafficid
sudo suricata-update

Suricata: Мета параметры

Мета-параметр (Meta Keywords) – оказывают влияние на представление правил.

- msg (message) – текстовая информация о сигнатуре
- sid (signature ID) – номер сигнатуры
- rev (revision) – версия
- gid (group ID) – номер группы
- classtype – используется для классификации
- reference – ссылка (“CVE-2021-2121” cve.mitre.org)
- priority – приоритет (число от 1 до 255)
- target – помогает описывать атаку
- metadata – дополнительная информация

Основные виды СЗИ

Suricata: Примеры

FIN-сканирование:
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"FIN_SCAN";
flow:stateless; flags:F; classtype:attempted-recon;)

Незашифрованный трафик на 443 порту:
alert tcp $EXTERNAL_NET any -> $HOME_NET 443 (msg:"Non-TLS on
TLS port"; flow:to_server; app-layer-protocol:!tls;)

Основные виды СЗИ

Suricata: Пример CVE-2020-8271

Позволяет атакующему выполнить произвольный код на Citrix SD-WAN Center.

Любой пользователь может загрузить и выполнить файл при помощи обхода каталогов (Path Traversal vulnerability).

alert http any any -> any any (msg:"Exploit CVE-2020-8271 on Citrix SD-WAN Center"; flow:to_server,established; content:"POST"; http_method; content:"/:///?/collector/licensing/upload"; http_raw_uri; reference:cve,CVE-2020-8271; classtype:web-application-attack; sid:20208271; rev:1;)

Suricata: Полезные ссылки

https://suricata.readthedocs.io/en/latest/quickstart.html - Документация к Suricata

https://suricata.readthedocs.io/en/suricata-6.0.10/rules/index.html - Раздел про правила Suricata

https://coralogix.com/blog/writing-effective-suricata-rules-for-the-sta/ - Советы по написанию правил

https://www.digitalocean.com/community/tutorials/understanding-suricata-signatures - Статья про правила Suricata

https://doc.emergingthreats.net/bin/view/Main/SidAllocation - Про распределение sid-идентификаторов правил

https://www.malware-traffic-analysis.net/ - Сайт с образцами трафика с ВПО для тренировки написания правил

https://www.youtube.com/watch?v=TApEp6SjlCg - Настройка Suricata в режиме IPS

Основные виды СЗИ

WIndows Defender (Windows Security)

Включение Windows Defender на вашем компьютере является важным шагом для обеспечения его безопасности. Инструкции о том, как включить Windows Defender и настроить его для максимальной защиты.

Шаг 1: Откройте «Настройки» Windows 10, нажав на значок «Пуск» в левом нижнем углу экрана и выбрав «Настройки» в меню. Вы также можете использовать сочетание клавиш Win + I для быстрого доступа к «Настройкам».

Шаг 2: В открывшемся окне «Настройки» выберите раздел «Обновление и безопасность».

Шаг 3: В левой панели выберите «Windows Defender», а затем перейдите на вкладку «Windows Defender». Здесь вы можете включить защиту в режиме реального времени, а также выполнить другие настройки для Windows Defender.

Основные виды СЗИ

Проверка активации Windows Defender

Чтобы убедиться, что Windows Defender правильно активирован и функционирует на вашем компьютере, выполните следующие шаги:

- Нажмите клавишу «Пуск» в левом нижнем углу экрана и выберите «Настройки» (иконка шестеренки).
- В открывшемся окне «Настройки» выберите «Обновление и безопасность».
- На левой панели выберите вкладку «Безопасность Windows».
- На главной панели в разделе «Защитник Windows» убедитесь, что статус говорит о том, что ваш компьютер защищен. Если статус указывает на то, что защитник отключен, необходимо нажать на ссылку «Управление настройками» и включить Real-time protection (Защиту в режиме реального времени).
- После включения Real-time protection (Защиту в режиме реального времени) статус должен измениться на «Включен» и указывать на то, что ваш компьютер защищен.

Основные виды СЗИ

Отключение антивирусов третьих сторон

Для отключения антивируса третьей стороны и включения Windows Defender следуйте инструкциям ниже:

- Откройте Панель управления Windows и выберите пункт «Система и безопасность».
- В разделе «Безопасность и обновление» выберите «Центр обеспечения безопасности».
- В левой части окна выберите пункт «Защита от вредоносных программ».
- В списке антивирусных программ найдите ваш антивирус третьей стороны и выберите его.
- В открывшемся окне выберите пункт «Отключить» или «Выключить».
- Подтвердите свое решение и закройте все окна.

Основные виды СЗИ

Планирование регулярных сканирований

Вот как настроить регулярные сканирования в Windows Defender:

- Войдите в настройки Windows Defender. Для этого откройте «Параметры» и выберите «Обновление и защита».
- В левой части окна выберите «Windows Defender».
- В разделе «Выбор режима работы» найдите опцию «План сканирования» и нажмите на ссылку «Настроить план сканирования».
- В открывшемся окне нажмите на кнопку «Добавить план» для создания нового плана сканирования.
- Введите имя для нового плана сканирования и выберите тип сканирования: «Полный», «Быстрый» или «Пользовательский».
- Если вы выбрали тип сканирования «Пользовательский», укажите папки или файлы, которые вы хотите включить в сканирование.
- Выберите дни и время, когда вы хотите, чтобы сканирование выполнялось автоматически. Вы можете выбрать несколько дней и указать время начала сканирования.
- Нажмите «Сохранить» для применения настроек.

Основные виды СЗИ

Защита электронной почты

Защита электронной почты — это комплекс мер и продуктов по защите элементов электронной почты от спама, фишинга, и вредоносных программ.

Основные угрозы, с которыми можно встретиться при эксплуатации сервера электронной почты:

- вредоносные программы;
- фишинг;
- спам.

Основные виды СЗИ

Защита электронной почты

Для обеспечения защиты корпоративной электронной почты следует придерживаться нескольких рекомендаций:

- Разместить почтовый сервер организации на границе сети либо в демилитаризованной зоне. Так при работе соответствующего программного обеспечения сервер будет фильтровать весь трафик на наличие спама и вирусов, отправляя во внутреннюю сеть компании только проанализированные данные.
- Защищать не только внешнюю (как входящую, так и исходящую) почту, но и внутреннюю почту организации. Если вдруг произойдет заражение, оно может распространиться через канал внутренней почты посредством доступа к адресной книге сотрудников.
- Запускать периодические антивирусные проверки архивов электронной почты. Это позволит избежать случаев, когда вирус попал в почтовый архив до того, как антивирусное решение смогло его идентифицировать.
- Выбирать средство для защиты электронной почты в соответствии с уровнем конфиденциальности обрабатываемой и хранимой информации.

Основные виды СЗИ

Защита электронной почты - Список средств

FortiMail - комплексное средство защиты электронной почты центра обработки данных

Kaspersky Total Security для бизнеса выступает в качестве решения комплексной защиты инфраструктуры компании, и способно обеспечить безопасностью каждый отдельный аспект вашей корпоративной сети. (KSMG)

UserGate Mail Security обеспечивает комплексную безопасность использования электронной почты в организации.

BI.ZONE Cloud Email Security & Protection позволяет защитить электронные почтовые ящики сотрудников компаний от спама, фишинга и вредоносных программ.

КАК ЗАЩИТИТЬ СВОИ ПОЧТОВЫЕ СЕРВЕРА?

Рекомендация № 1.
Использовать механизмы проверки PTR-записи почтовых сервисов.
PTR-запись – это DNS запись, предназначенная для преобразования IP-адреса в доменное имя. Чаще всего PRT-запись представляются как обратную A-запись. Данный механизм проверки является базовым, предназначен для защиты почтовых серверов организации от спама и фишинговых атак, использующих мошеннические домены.

При получения заголовка любого электронного письма почтовый сервер получателя находит IP-адрес почтового сервера отправителя в заголовке и запрашивает доменное имя отправителя по указанному IP-адресу.
Искомое доменное имя можно получить только в случае если для анализируемого IP-адреса существует PTR-запись. Далее, полученное в результате запроса доменное имени сверяется с доменным именем из заголовка электронного письма. В случае если доменные имена совпадают, то считается, что проверка прошла успешно. Подробно указанная процедура описана в RFC 2505 и поддерживается всеми современными почтовыми серверами (Exim, Postfix, Sendmail, Microsoft Exchange Server, MDaemon Server и другие) .

КАК ЗАЩИТИТЬ СВОИ ПОЧТОВЫЕ СЕРВЕРА?

Рекомендация № 2

Использовать механизмы шифрования почтовых сообщений и (или) передачу почтовых сообщений с использованием криптографических протоколов передачи данных (SMTPS, STARTTLS).

SMTPS – это криптографический метод защиты протокола SMTP путем создания неявного TLS-соединения на 465 порту транспортного уровня. STARTTLS – это расширение протокола SMTP, позволяющее создать зашифрованное соединение прямо поверх обычного TCP-соединения на стандартном порту обмена почтовыми сообщениями (25 порт).

КАК ЗАЩИТИТЬ СВОИ ПОЧТОВЫЕ СЕРВЕРА?

Рекомендация № 3

Использовать механизмы проверки SPF-записи почтовых сервисов. SPF (Sender Policy Framework) – это расширение (дополнение) для протокола отправки почты через SMTP-сервер, реализующее механизм 3 подтверждения отправителя по IP-адресу. В настоящее время существует две версии расширения: SPFv1 и SPFv2.0/mfrom,pra.

Версия расширения SPF2.0/mfrom,pra также называемая Sender ID не получила широкого распространения. Данные механизм проверки предназначен для поддержания репутации организации путем защиты электронных писем от подмены поля «Отправитель» (From)

КАК ЗАЩИТИТЬ СВОИ ПОЧТОВЫЕ СЕРВЕРА?

Рекомендация № 4

Использовать механизмы почтовой аутентификации отправителя почтовых сообщений (DKIM).

DKIM (DomainKeys Identified Mail) – это расширение (дополнение) для протокола отправки почты через SMTP-сервер, реализующее механизм электронной цифровой подписи электронного письма. Указанный механизм проверки предназначен для поддержания репутации организации путем защиты электронных писем от подмены отправителя

КАК ЗАЩИТИТЬ СВОИ ПОЧТОВЫЕ СЕРВЕРА?

Рекомендация № 5

Обеспечить фильтрацию почтовых сообщений с использованием списков нежелательных отправителей почтовых сообщений.

Указанная рекомендация предназначена для защиты от спама и фишинговых атак, использующих легитимные доменные имена или IP-адреса

КАК ЗАЩИТИТЬ СВОИ ПОЧТОВЫЕ СЕРВЕРА?

Рекомендация № 6

Обеспечить в реальном масштабе времени автоматическую антивирусную проверку файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных вредоносного ПО.

Данная рекомендация предназначена для обнаружения, блокировки и удаления электронных писем с вложениями содержащими в себе вредоносное программное обеспечение

КАК ЗАЩИТИТЬ СВОИ ПОЧТОВЫЕ СЕРВЕРА?

Рекомендация № 7

Блокировать массовую рассылку почтовых сообщений. Указанная рекомендация предназначена для защиты защиты репутации организации, отправляющей большое количество почтовых сообщений, а также обеспечения доступности почтового сервера организации

При начальной конфигурации почтового сервера отправителя необходимо задать разрешенное количество отправляемых электронных писем в единицу времени (чаще всего в 1 мин). При превышении данного параметра электронные почтовые сообщения будут помещаться в очередь до возможности отправки.

Teach
Me
Skills

Спасибо за внимание!