УДК 004.681.5

АНАЛИЗ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ АКТИВНЫХ СРЕДСТВ СЕТЕВОЙ БЕЗОПАСНОСТИ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Волхонский А.Н.[1]
[1]*ФГБОУ ВО «Самарский государственный технический университет», Самара, e-mail: avolhonskij34@gmail.com*
Чупринина А.С.[1]
[1]*ФГБОУ ВО «Самарский государственный технический университет», Самара, e-mail: anna.chuprinina.02@mail.ru*
Падучих Д.В.[1]
[1]*ФГБОУ ВО «Самарский государственный технический университет», Самара, e-mail: dasha-oleinikova2002@mail.ru*

Была рассмотрена проблематика обеспечения информационной безопасности конфиденциальной информации с использованием интеллектуальных средств защиты. вопрос, связанный с активными средствами защиты технически сложных объектов Далее были рассмотрены активные средства сетевой безопасности, а именно: IPS – Системы предотвращения вторжений; NGFW – Межсетевые экраны нового поколения; SWG– Шлюзы информационной безопасности; AMP – расширенная защита от вредоносных программ; DLP– Системы предотвращения утечки данных; Рассмотрены их развёртывания на базе Bypass и брокеров сетевых пакетов для обеспечения гарантированной безопасности сети, а также компании, которые производят средства безопасности в этой области. Рассматриваются характеристики в сравнении с предыдущим поколением, в новых устройствах добавлена тесная интеграция дополнительных возможностей, таких как встроенная глубокая проверка пакетов. Рассматриваются средства активной безопасности, подключаемые «в разрыв», которые не только обнаруживают угрозы, но и блокируют их в режиме реального времени. Описываются системы предотвращения вторжений и их принцип действия, предназначенные для обнаружения и предотвращения попыток несанкционированного доступа к конфиденциальным данным, повышения привилегий, использования уязвимостей программного обеспечения и вывода из строя компьютерных систем.

Ключевые слова: активная защита, технически сложный объект, автоматизация, защита информации.

ANALYSIS THE POSSIBILITY OF APPLYING ACTIVE NETWORK SECURITY TOOLS TO ENSURE INFORMATION PROTETION OF AUTOMATED SYSTEMS

Volkhinskij A.N.[1]
[1]*Samara State Technical University, Samara, e-mail: avolhonskij34@gmail.com*
Chuprinina A.S.[1]
[1]*Samara State Technical University, Samara, e-mail: anna.chuprinina.02@mail.ru*
Paduchikh D.V.[1]
[1]*Samara State Technical University, Samara, e-mail: dasha-oleinikova2002@mail.ru*

The problem of ensuring the information security of confidential information using intellectual means of protection was considered. a question related to active means of protecting technically complex objects Next, active means of network security were considered, namely: IPS - Intrusion Prevention Systems; NGFW - Next Generation Firewalls; SWG - Information Security Gateways; AMP - Advanced Malware Protection; DLP – Data Leak Prevention Systems; Their deployments based on Bypass and network packet brokers to ensure guaranteed network security, as well as companies that produce security tools in this area, are considered. Reviewing performance over the previous generation, the new devices add tight integration of additional features such as built-in deep packet inspection. Active security tools are considered, connected "into the gap", which not only detect threats, but also block them in real time. Describes intrusion prevention systems and their principle of operation, designed to detect and prevent unauthorized access to confidential data, privilege escalation, exploitation of software vulnerabilities and disable computer systems.

Keywords: active protection, technically complex object, automation, information security.

Активные средства сетевой безопасности

Средства активной безопасности, подключаемые «в разрыв» (in-line), не только обнаруживают угрозы, но и блокируют их в режиме реального времени. При внедрении активных средств специалисты сталкиваются с проблемами обеспечения отказоустойчивости сети, дальнейшей масштабируемости средств безопасности, а также с необходимостью уменьшения задержек передачи пакетов при увеличении объёма трафика в сети.

Среди наиболее популярных активных средств информационной безопасности остановимся на;

1. IPS – Системы предотвращения вторжений;
2. NGFW – Межсетевые экраны нового поколения;
3. SWG– Шлюзы информационной безопасности;
4. AMP – расширенная защита от вредоносных программ;
5. DLP– Системы предотвращения утечки данных;
6. Anti-DDoS - Системы предотвращения распределённого отказа в обслуживании.

Рассмотрим способы их развёртывания на базе Bypass и брокеров сетевых пакетов для обеспечения гарантированной безопасности сети.

Системы предотвращения вторжений (IPS)

Системы предотвращения вторжений (IPS) — это программные и аппаратные средства, предназначенные для обнаружения и предотвращения попыток несанкционированного доступа к конфиденциальным данным, повышения привилегий, использования уязвимостей программного обеспечения и вывода из строя компьютерных систем. Такие попытки вторжений осуществляются главным образом через Интернет или локальную сеть, могут иметь форму атак хакеров/инсайдеров или же быть результатом действий вредоносных программ.

IPS — это логическая эволюция IDS. Однако если IPS заблокировала «хороший» трафик, который, как она подозревала, был «плохим» (ложное срабатывание), или же физически вышла из строя, нарушив целостность сети, то важные бизнес-процессы компании нарушатся. Таким образом, специалисты по ИБ должны тщательно выбирать и развёртывать IPS с большой осторожностью.

Схема работы IPS системы представлена на рисунке 1.

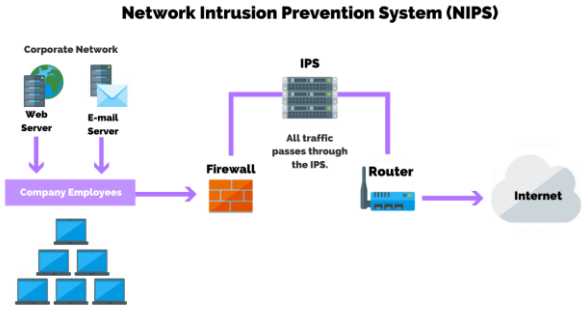

Рисунок 1 – Схема работы IPS

В настоящее время системы IPS активно развиваются в части сокращения числа ложных срабатываний и увеличения эффективности решения. Результатом усовершенствования можно считать так называемые IPS-системы нового поколения - NGIPS, которые выполняют все функции в режиме реального времени, никак не влияя на сетевую

активность организации, и, помимо всего прочего, предоставляют возможности мониторинга приложений и использования информации из сторонних источников.

В пространстве IPS решений представлены продукты следующих производителей: PositiveTechnologies, Код Безопасности, Smart-Soft, InfoWatch, Инфотекс, Stonesoft, TrendMicro, Fortinet, Cisco, HP, IBM, Juniper, McAfee, Sourcefire, Stonesoft, TrendMicro, CheckPoint, PaloAltoNetworks.

Межсетевые экраны нового поколения (NGFW)

Межсетевые экраны нового поколения (Next-GenerationFirewall - NGFW) — это эволюция типовых межсетевых экранов с возможностью отслеживания состояния соединений. Поскольку всё большее число компаний сейчас используют онлайн-приложения и службы SaaS, то классический контроль портов и протоколов уже недостаточен для обеспечения эффективной сетевой безопасности.

Схема работы NGFW системы представлена на рисунке 2.

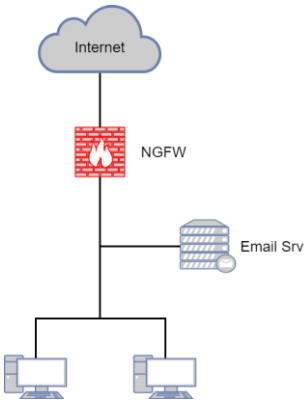

Рисунок 2 – Схема работы NGFW

В отличие от предыдущего поколения, в новых устройствах добавлена тесная интеграция дополнительных возможностей, таких как встроенная глубокая проверка пакетов (DPI), предотвращение вторжений (IPS) и проверка трафика на уровне приложений. Некоторые NGFW также включают проверку зашифрованного трафика TLS/SSL, фильтрацию веб-сайтов, управление пропускной способностью, QoS, антивирусную проверку и интеграцию со сторонними системами управления идентификацией (LDAP, RADIUS и ActiveDirectory). Решения NGFW в скором времени заменят традиционные межсетевые экраны, предотвращая вторжения и контролируя приложения как по периметру, так и внутри сети.[1]

Производители NGFW решений: UserGate, Континент, Huawei, CheckPoint, Cisco, Fortinet, McAfee, PaloAltoNetworks и Sourcefire.

Шлюзы информационной безопасности (SWG)

Прокси-серверы с функциями информационной безопасности (Security Web Gateway — SWG), также известные как веб-фильтры — это программно-аппаратные комплексы (ПО + сервер), разработанные и оптимизированные для соблюдения политик веб-безопасности компании и контроля доступа пользователей к веб-сайтам. Веб-сайты, которые содержат вредоносное ПО или неприемлемый контент (например, порнографию или азартные игры), блокируются на SWG, тем самым повышая производительность труда сотрудников, ограничивая ответственность компании и защищая компьютерные устройства пользователей от вреда.

Схема работы SWG системы представлена на рисунке 3.

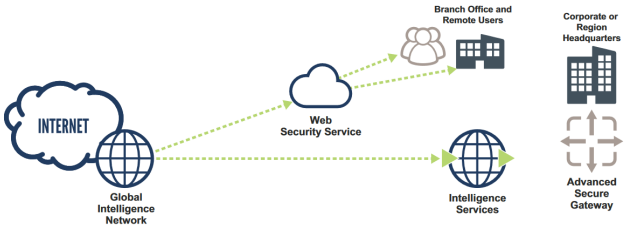

Рисунок 3 – Схема работы SWG

Поставщики SWG группируют веб-сайты по категориям и выпускают обновления безопасности, как правило, на ежедневной основе. Администраторы SWG могут создавать политики доступа на основе категорий веб-сайтов и относить их к отдельным пользователям и группам пользователей.[2]

Производители SWG решений: Ростелеком-Солар, Smart-Soft, UserGate, ESET, Kaspersky, Sophos, TRENDmicro, Huawei, Blue Coat, Cisco, McAfee, Trustwave и Websense.

Расширенная защита от вредоносных программ (AMP)

Традиционные решения безопасности, такие как системы предотвращения вторжений, антивирусные продукты и шлюзы информационной безопасности предназначены для обнаружения известных угроз и эксплойтов, нацеленных на определённые уязвимости операционных систем и приложений. Однако сегодня уязвимости нулевого дня (Zero-DayExploit - атаки, нацеленные на уязвимости, для которых ещё не разработана защита) вызывают наибольшую озабоченность компаний и правительственных учреждений.[3]

Для защиты от этих угроз существует категория решений сетевой безопасности - AMP (AdvancedMalwareProtection). Основная задача AMP – проверка файла, пересылаемого через сетевое устройство и/или записываемого на конечное оборудование, на наличие вредоносного кода. Система AMP осуществляет ретроспективный анализ и обеспечивает защиту не только до момента атаки или во время атаки, но и после того, как атака прошла. Кроме того, это решение позволяет отследить все пути распространения файла и может заблокировать файл на уровне сети. Схема работы SWG системы представлена на рисунке 4.

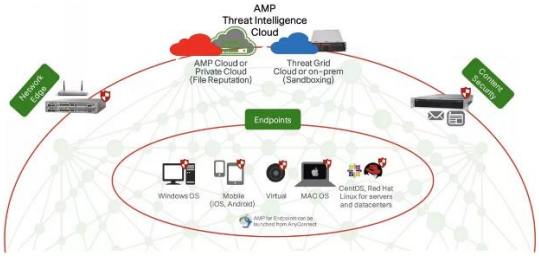

Рисунок 4 – Схема работы AMP

Производители AMP решений: Kaspersky, Malwarebytes, Cisco, Damballa, FireEye и Palo Alto Networks.

Системы предотвращения утечки данных (DLP)

Системы предотвращения утечки данных (DataLossPrevention или DataLeakagePrevention - DLP) — это программно-аппаратные комплексы (ПО + сервер), которые предназначены для обнаружения и предотвращения потенциальных нарушений конфиденциальности данных и личной информации (номера кредитных карт, номера телефонов, данные паспорта и т. д.) путём мониторинга данных в нескольких состояниях:

1. при использовании (Data-in-Use) — на рабочем месте пользователя;
2. при передаче (Data-in-Motion) — в сети компании;
3. при хранении (Data-at-Rest) — на серверах и рабочих станциях компании;

Производители DLP решений: InfoWatch, ИнфосистемыДжет, SmartLineInc, Гарда Технологии, Zecurion, Ростелеком-Солар, Falcongaze, Атом Безопастность, ESET, SearchInform, CoSoSys, BlueCoat, CheckPoint, Cisco (IronPort), Fidelis, McAfee, RSA, Verdasys, Symantec, Websense.[4]

Системы предотвращения распределённого отказа в обслуживании

Системы предотвращения распределённого отказа в обслуживании (DistributedDenialofService (DDoS) Protection или Anti-DDoS) — это специализированные программно-аппаратные и программные средства, предназначенные для защиты веб-серверов/сайтов компании от распределённых атак типа «Отказ в обслуживании».

Атака типа «отказ в обслуживании» (DoS) - это попытка одного компьютера сделать другой компьютер недоступным для его предполагаемых пользователей путём «забивания» его полосы пропускания и/или вычислительных ресурсов паразитным трафиком, часто через поток пакетов SYN или ICMP. Распределённый отказ в обслуживании (DDoS) — это DoS-атака, инициируемая ботнетом (совокупностью компьютеров, называемых ботами, которые заражены зомби-агентами или троянами), обычно используется для атак на целевые веб-сайты. На предприятиях системы Anti-DDoS помогают выявлять и предотвращать DDoS-атаки путём использования проприетарных алгоритмов и оценки механизмов защиты.

Средства безопасности в этой области производят компании: DDOS-GUARD, СТОРМ СИСТЕМС, Variti, Гарда Технологии, Kaspersky, InoventicaTechnologies, QratorLabs, AkamaiTechnologies, CloudFlare, Imperva, Sucuri, F5 Networks, ArborNetworks, Cisco, Corero и VeriSign.[5]

Список литературы

1) Защита информации в информационных системах и компьютерных сетях [Электронный ресурс]// Национальный открытый университет ИНТУИТ // URL: https://intuit.ru/studies/courses/13845/1242/lecture/27503

2) Ю.А. Гатчин, Е.В. Климова ВВЕДЕНИЕ В КОМПЛЕКСНУЮ ЗАЩИТУ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ [Электронный ресурс]// Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики // URL: https://books.ifmo.ru/file/pdf/2006.pdf

3) Наиболее распространенные угрозы [Электронный ресурс]// Национальный открытый университет ИНТУИТ //URL: https://intuit.ru/studies/courses/10/10/lecture/300?page=1

4) Средства защиты информации (СЗИ) [Электронный ресурс]// Защита информации/ Департамент цифрового развития Смоленской области // URL: https://it-security.admin-smolensk.ru/zinfo/szi/

5) Пассивные и активные методы и способы защиты каналов утечки информации [Электронный ресурс]//studfile// URL:https://studfile.net/preview/5868802/