Калашников Кирилл Юрьевич,

студент, МГТУ им. Г.И. Носова, г. Магнитогорск;

Баранкова Инна Ильинична,

заведующая кафедрой ИиИБ, профессор, доктор технических наук, аккредитованный эксперт РосОбрНадзора, член Координационного совета по подготовке кадров в области информационной безопасности по УРФО Носова, г. Магнитогорск

АНАЛИЗ СОСТОЯНИЯ ЛВС ПРЕДПРИЯТИЯ И РАЗРАБОТКА КОМПЛЕКСА МЕР ПО ЕЕ МОДЕРНИЗАЦИИ

Аннотация. В данной статье рассмотрены актуальные для всех организаций проблемы, связанные с сетью, критические ошибки при ее построении. В частности, описана существующая сеть предприятия. Также рассмотрены основные угрозы, связанные с сетевыми атаками и недобросовестностью сотрудников предприятия.

Ключевые слова: информация, безопасность, локальные вычислительные сети, угрозы, сетевые атаки.

В современном мире, наполненном информацией, каждая организация использует компьютерную технику, соединенную в сеть. Каждое устройство может получить доступ к любому узлу, что одновременно невероятно облегчает работу, но и создает массу возможных проблем и угроз, связанных с работой в сети.

Для качественной, быстрой и безопасной работы каждая сеть должна соответствовать ряду критериев:

1. Должен присутствовать сетевой экран на точке входа в ЛВС. Сетевой экран — самая важная часть защиты сети от сетевых атак извне. В качестве примера атак можно привести сетевую разведку, позволяющую определить имена хостов в сети и их DNS-имена; сканирование портов, позволяющее определить список поддерживаемых хостами

услуг; анализ характеристик приложений, который определяет, какие характеристики используются приложениями, что позволяет спланировать сетевую атаку и взлом хоста; парольные атаки, то есть подбор паролей к хостам, к примеру, с использованием брутфорса, а также многие другие.

2. Для предотвращения потерь бизнеса от кражи информации вследствие сетевых атак сетевой экран должен быть правильно настроен, в частности, необходимо закрыть большинство портов для доступа извне, отбрасывать попытки подключиться к сети более нескольких раз подряд, заносить адреса, с которых поступают такие попытки, в черный список.

3. Должно присутствовать разграничение доступа внутри сети. Недобросовестные и негативно настроенные по отношению к организации сотрудники, а также посторонние, получившие физический доступ к какому-либо устройству, входящему в ЛВС, могут попытаться получить служебную информацию с другого узла в сети, которая может повредить репутации предприятия, или заставить его понести финансовые потери. Для предотвращения данных информационных потерь необходимо разделить ЛВС на несколько логических частей, каждая из которых не сможет взаимодействовать с другими. Для обмена информацией между такими частями должен существовать общий узел обмена информацией, а данные, специфичные для каждого отдела, останутся внутри соответствующей части сети. Для разделения сети используется технология VLAN, позволяющая на сетевом уровне разбить ЛВС на логические части.

4. Для предотвращения ситуации, когда злоумышленник захочет заставить сеть выдать отказ в обслуживании, проще говоря, занять весь свободный канал, и нагрузить до отказа сетевое оборудование, необходимо использование технологии QoS, позволяющее ограничить процент использования

пропускной способности сети одним узлом;

5. Необходимо использовать надежное сетевое оборудование. В погоне за экономией многие организации используют дешевое и ненадежное сетевое оборудование, что может повлечь за собой отказ большого сегмента сети, на восстановление доступа к которого может уйти очень много времени, что является особенно критичным в бизнесе по работе с клиентами, которые не будут ждать, а просто уйдут к конкуренту, что влечет репутационные и финансовые потери;

6. На конечных узлах в сети необходимо использование антивирусного программного обеспечения, которое защищает ЛВС от распространения вирусов, программ-шпионов и прочих. Одной из самых страшных угроз является присутствие в сети вируса, который распространяется по узлам, нарушая работу предприятия. При использовании ненадежного антивирусного ПО любой сотрудник по незнанию или злому умыслу может занести в сеть вредоносную программу, на борьбу с которой у ИТ-специалистов могут уйти дни и недели. Особенно важно, чтобы подобные программы не проникли в административную часть сети, на серверы, имеющие доступ ко всей ЛВС.

7. В качестве примера модернизации существующей ЛВС рассмотрим кинотеатр, в котором сетевой безопасности не уделялось достаточное внимание, а именно, присутствовали все вышеперечисленные проблемы:

1. Отсутствовал сетевой экран, в качестве маршрутизатора использовалась дешевая модель, предназначенная преимущественно для домашнего использования;

2. Отсутствовало разграничение доступа внутри сети

3. Использовалось дешевое и ненадежное сетевое оборудование

4. Использовался бесплатный антивирус, который мог

выключить любой сотрудник у себя на компьютере.

Как итог, периодически предприятие сталкивалось с недобросовестностью сотрудников, на сеть совершались систематические атаки, как извне, так и изнутри. Также в 2017 году организация столкнулась с вредоносной программой, названной “Petya”, которая распространилась по сети, что повлекло за собой паралич работы всего предприятия, вследствие чего были понесены большие финансовые и репутационные потери, после чего руководство задумалось о сетевой безопасности и создании полноценного ИТ-отдела.

Результатом работы ИТ-специалистов стал выбор нового сетевого оборудования, закуплены новый маршрутизатор, настроен сетевой экран, закуплены коммутаторы уровня L2+, настроены VLAN, QoS, VPN, закуплен и настроен корпоративный антивирус, отслеживающий состояние всех узлов в сети.

Проблема сетевой безопасности остро стоит в современном мире, так как ни одно предприятие сейчас не обходится без использования компьютеров и сетей. Необходимо пристально следить за состоянием сети, не экономить на ИТ-инфраструктуре и специалистах.

СПИСОК ЛИТЕРАТУРЫ

1. Мазнин Д.Н., Баранкова И.И., Михайлова У.В., Афанасьева М.В. Организация защиты данных в вычислительных сетях. Лабораторный практикум: Учебное пособие. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2018. – 54 с.

2. Михайлова У.В., Ершов В.А. Способы организации и методы противодействия DOS/DDOS – атакам // Безопасность информационного пространства: сборник трудов XIII Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных. Министерство образования и науки Российской Федерации, Южно-Уральский государственный университет, Кафедра «Безопасность информационных систем». – 2015. – С. 73-79.