УДК 004.056

РАЗРАБОТКА МЕТОДОВ ПОВЫШЕНИЯ СТЕПЕНИ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ КИИ НА ПРИМЕРЕ ОБОРУДОВАНИЯ CISCO.

Галецкая А.В.
Научный руководитель – Профессор Лившиц И.И.
Санкт-Петербург, Университет ИТМО

В данной работе представлены результаты анализа критических уязвимостей распространенного оборудования компании Cisco. Представлены результаты оценки рисков для выбранных уязвимостей и сформулированные меры безопасности.

Введение.

Общеизвестно, что информация в наше время хранится преимущественно в цифровом виде, и очень важно обеспечить ее безопасность, особенно в отношении объектов критической информационной инфраструктуры (КИИ). Также достаточно известно, что к какой бы сфере ни относился тот или иной объект КИИ, зачастую всем им необходимы сети и телекоммуникационные технологии.

Оборудование компании Cisco весьма распространено на российском рынке, а на мировом и вовсе занимает наибольшую долю рынка телекоммуникационного оборудования. Такая крупная компания, вне сомнения, прикладывает много усилий для обеспечения безопасности своих продуктов, однако исследования показывают, что несмотря на широкие возможности больших компаний, их продукты зачастую имеют большое количество уязвимостей, что относится и к компании Cisco в том числе.

Основная часть.

Данное исследование было начато со сбора данных об уязвимостях распространенного оборудования компании Cisco, а именно о критических уязвимостях, которые были найдены за последние два года. Всего была найдена тридцать одна уязвимость для четырех категорий оборудования. Критичность уязвимостей определялась по метрике NIST и выставленному базовому CVSS значению. Далее были собраны данные о временном промежутке между датой нахождением уязвимости и датой выхода исправленной версии. Несмотря на то, что не для всех уязвимостей есть подобные данные, было определено, что для исправления уязвимости может потребоваться от двух дней до нескольких месяцев, что подтверждает необходимость разработки дополнительных мер защиты.

Далее для полученных данных была проведена оценка риска в соответствии со стандартом ИСО 27005, которая состояла из определения угрозы; риска; решения, принятого в соответствии с моделью 4Т; предлагаемых мер безопасности; остаточного риска для выбранных мер; финального решения.

После проведения анализа уязвимостей, были выявлены самые распространенные угрозы: несанкционированное использование оборудования, фальсификация прав, незаконная обработка данных, отказ в осуществлении действий и раскрытие данных.

Далее после выявления рисков была выполнена основная часть плана работы – разработка мер безопасности. Для каждой конкретной уязвимости были сформулированы все возможные меры, обеспечивающие защиту, после чего они сравнивались. Основные меры, которые оказались наиболее подходящими с точки зрения простоты реализации, стоимости и времени, включают в себя: замену уязвимого оборудования; реализацию второй линии; временное внедрение белого списка IP адресов и ACL и ожидание обновления; внедрение обновления и внесение рекомендованных изменений в конфигурацию; временное отключение программного обеспечения или функции на короткий период времени и установка обновления, которое либо уже вышло, либо обещано к выпуску через несколько дней;

временное отключение ПО до выпуска и внедрения обновления, если ПО не критично для работы компании.
Из предложенных решений, считая относительно количества исправленных уязвимостей, самым распространенным оказалось временное отключение функции на время установки патча, что, по сути, относится к случаям, когда уже существует доступная безопасная версия и когда уязвимости можно эксплуатировать только в случае отсутствия последнего обновления, что, впрочем, не является редкостью. Следующей мерой стала замена уязвимого оборудования – в основном поскольку для ряда устаревшего оборудования, для которого уже не планируются обновления, было найдено достаточно большое количество уязвимостей. Третьей по распространенности мерой стало временное внедрение белого списка IP адресов и ACL и дальнейшее ожидание обновления, поскольку данное решение является достаточно дешевым и в то же время действенным, так как большинство уязвимостей предполагают удаленный доступ атакующего.
Решения, подобные выделенным, будучи введенными в политику безопасности компании, помогут противостоять возможным атакам на телекоммуникационные системы через уязвимости сетевого оборудования.

Выводы.
В ходе данного исследования были собраны данные по критическим уязвимостям оборудования Cisco, обнаруженных за два года, проведена оценка рисков в соответствии со стандартом ИСО 27005. В ходе оценки рисков были выявлены угрозы, описаны возможные риски и выбраны меры безопасности.
Общие результаты данной работы позволили определить комплекс решений, которые в дальнейшем будут взяты за основу методики повышения защищенности объектов КИИ. Эффективность выбранных мер была определена через оценку разницы между изначальным и остаточным риском.
Далее планируется продолжение исследования стандартов и регламентов КИИ, связь разработанных мер безопасности с ними, таким образом формулируя методологию повышения защиты безопасности объектов КИИ, работающих на оборудовании Cisco. Сама методология может быть применена для любых компаний, работающих на оборудовании Cisco, которые либо относятся к критической информационной инфраструктуре, либо хотят иметь хороший уровень информационной безопасности, даже не будучи обязаны к этому по закону.