ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF EDUCATION AND SCIENCE
OF THE REPUBLIC OF KAZAKHSTAN

Л.Н. ГУМИЛЕВ АТЫНДАҒЫ
ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ
ЕВРАЗИЙСКИЙ НАЦИОНАЛЬНЫЙ
УНИВЕРСИТЕТ ИМ. Л.Н. ГУМИЛЕВА
GUMILYOV EURASIAN
NATIONAL UNIVERSITY

ЖАС ҒАЛЫМДАР КЕҢЕСІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2015» атты X Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ X Международной научной конференции студентов и молодых ученых «Наука и образование - 2015»

PROCEEDINGS of the X International Scientific Conference for students and young scholars «Science and education - 2015»

УДК 001:37.0
ББК72+74.04
Ғ 96

Ғ96
«Ғылым және білім – 2015» атты студенттер мен жас ғалымдардың X Халық. ғыл. конф. = X Межд. науч. конф. студентов и молодых ученых «Наука и образование - 2015» = The X International Scientific Conference for students and young scholars «Science and education - 2015». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie-2015/, 2015. – 7419 стр. қазақша, орысша, ағылшынша.

ISBN 978-9965-31-695-1

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001:37.0
ББК 72+74.04

ISBN 978-9965-31-695-1

©Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2015

УДК 004.41/42

ИНДУСТРИАЛЬНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ В УСЛОВИЯХ ВОЗРОСШИХ КИБЕРУГРОЗ

Ахметова Жанар Жумановна
zaigura@mail.ru
Докторант 1-курса специальности «6D070300-Информационные системы»
ЕНУ им. Л.Н.Гумилева, Астана, Казахстан
Научные руководители –С.Н.Боранбаев, С.С.Жузбаев

Кибератака — это попытка внести изменения в работу компьютерных систем или сетей, вывести их из строя, разрушить, а то и уничтожить информацию или программы, которые в них хранятся или какие они передают (Национальный научный совет США).

Один из самых распространенных на практике методов кибератак заключается в том, что злоумышленники для того, чтобы избежать обнаружения атакуют плохо защищенные компьютеры и прокси-сервера, а затем через них производят атаки по всему миру. Они научились осторожно тестировать защиту компьютеров и серверов так, чтобы это не было обнаружено системами безопасности и, найдя уязвимости, атакуют. Такие атаки практически всегда носят международный характер, но пока нет никаких международных ответных мер, что напрягает правоохранительные органы. Поэтому они стремятся к сотрудничеству со странами, где обычно находятся прокси-сервера, через которые происходят международные кибератаки [2].

Приведем примеры самых последних крупнейших кибератак на индустриальные системы управления:

- 2003 год. Компьютерный червь Slammer быстро распространился Интернетом, поразив приблизительно 75 000 компьютеров в общей сложности за 10 минут. Скорость Интернета упала почти до нуля, перестали работать банкоматы и немало веб-сайтов. Не могли взлететь самолеты, а на одной из атомных электростанций вышли из строя компьютеры и компьютеризованные системы безопасности.
- 2007 год. Серия кибератак была осуществлена на Эстонию. Они были направлены на компьютерные системы правительства, а также банковских учреждений и средств массовой информации. Большее число этих атак происходили из сетей (ботнетов), которые насчитывали свыше миллиона компьютеров в 76 странах. Все эти машины атаковали упомянутые мишени лавинами фальшивых запросов об информации.
- 2010 год.промышленные системы автоматизации тяжело пережили атаку уже широко известного компьютерного вируса Stuxnet. Высокотехнологичный компьютерный червь Stuxnet атаковал системы контроля над производственным процессом на атомной электростанции в Иране. Это событие было самым широко освещаемым в профильных СМИ, но не стало единственным, с того момента промышленные сети и системы стали одной из основных целей для кибератак.

Кибератаки на критически важные инфраструктуры встречаются сегодня все чаще и стали значительной проблемой для различных организаций по всему миру [3].

Критическая информационная инфраструктура - совокупность автоматизированных систем управления критическими важными объектами и обеспечивающих их взаимодействие информационно- телекоммуникационных сетей, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий.

Критически важный объект инфраструктуры - объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта

страны либо административно- территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок[1].

Электростанции, центры контроля движения транспорта, системы очистки воды и фабрики стали предметом внимания злоумышленников, постоянно подвергаясь сетевым взломам, кражам данных и атакам на отказ в обслуживании.

Уязвимости данных систем могут быть различными — от обычных ситуаций с отсутствием паролей и использованием учетных записей, созданных по умолчанию, и до проблем с конфигурациями или ошибок в программном коде. Поэтому как только хакер получает возможность запустить программу, имеющую доступ к контроллеру, вероятность успешного проведения атаки становится очень высокой.

В 2012 году немецкая энергетическая компания 50 Hertz стала жертвой кибератаки, которая вывела из строя систему интернет-коммуникаций. Это был первый подтвержденный пример цифрового нападения на европейского оператора энергосетей.

В 2001 некий австралиец был отправлен в тюрьму за взлом системы управления очистными сооружениями, который привел к сбросу миллионов литров неочищенных сточных вод в водоемы местных парков и реки.

Подобные атаки на критически важные инфраструктуры часто влияют на работу различных служб, целостность данных, и даже угрожают общественной безопасности. Также в результате атак системы перестают соответствовать требованиям регуляторов. Поэтому организациям нужно предпринимать определенные меры, чтобы предотвращать подобные проблемы с безопасностью[1].

Однако это возможно сделать только при понимании различий между ICS/SCADA и традиционными ИТ-средами. Даже если род деятельности промышленного предприятия не связан с критически важными процессами (энергетика, транспорт, оборонная промышленность), большинство технологических процессов автоматизировано с помощью SCADA (система диспетчерского управления и сбора данных) или типовых систем автоматического управления.

Критически важные инфраструктурные объекты (из сферы электроэнергетики, нефти и газа, водоснабжения, очистки отходов и т.д.) в значительной степени зависят от электрических, механических, гидравлических и других устройств. Это оборудование управляется и контролируется отдельными компьютерными системами — контроллерами и сенсорами. Данные системы подключаются к управляющим системами и создают сети SCADA (Supervisory Control and Data Acquisition — диспетчерское управление и сбор данных) и решения ICS (Industrial Control System — система производственного контроля). ICS и SCADA обеспечивают эффективный сбор и анализ данных и помогают автоматизировать контроль над оборудованием — насосами, клапанами, реле и т.д. Преимущества данных систем обусловили их широкое распространение. Надежность и стабильность SCADA и ICS позволяют использовать их на критически важных объектах в течение длительного времени.

Сети и устройства SCADA/ICS разрабатывались для того, чтобы обеспечить управляемость и контроль при максимальном уровне надежности. Часто они не обладают механизмами, призванными предотвратить неавторизованный доступ или способными справляться с растущими угрозами безопасности, широко распространенными в мире ИТ и исходящими как из внутренних, так и из внешних сетей.

Такие системы в последние годы стали подвержены атакам вредоносного ПО не меньше, чем «традиционные» финансовые и правительственные структуры. Отличие лишь в том, что атаки, направленные на промышленные системы, как правило, не регистрируются и их последствия обычно выглядят как сбои в работе, не связанные с действиями какого-либо вредоносного ПО.

И хотя их внедрение в большинстве случаев является коммерческой тайной, контроллеры SCADA фактически представляют собой маленькие компьютеры. Они

используют такие стандартные элементы, как операционные системы (часто встроенные Windows или Unix), программные приложения, учетные записи, протоколы передачи данных и так далее. Более того, во многих средах управления используются стандартные рабочие станции Windows и Unix.

В результате уже знакомые проблемы, связанные с уязвимостями и эксплойтами, оказываются применимы и к ICS и SCADA. Дополнительной проблемой является то, что все эти системы нередко располагаются в физически труднодоступных местах и должны находиться в рабочем режиме 24/7.

Существует типичное мнение, что сети ICS и SCADA физически отделены от корпоративных ИТ-сетей. И это может быть так, ведь некоторые компании используют отдельные сети или разделяют сети контроля и корпоративные ресурсы. В других случаях компании используют одни и те же инфраструктуры LAN и WAN, однако применяют шифрование для трафика ICS и SCADA при передаче в общей среде. Но чаще всего сети требуют наличия определенного уровня взаимодействия, чтобы получать операционные данные или экспортировать информацию в сторонние системы. Устройства из сетей SCADA имеют ряд особенных характеристик, которые могут сильно отличаться от традиционных ИТ-систем:

- Они часто устанавливаются в таких местах, куда сложно попасть физически (например, на башнях, нефтяных вышках, промышленном оборудовании), а также работают в значительно более сложных внешних условиях, чем обычные ИТ-системы (на улице, при экстремальных температурах и вибрациях) или требуют наличия специальных условий питания и монтажа;
- На них часто инсталлированы проприетарные операционные системы, в которых не предусмотрена возможность усиления безопасности;
- Невозможно часто обновлять или загружать исправления для ПО в связи с недопустимостью простоев, ограничениями доступа или необходимостью повторной сертификации ПО;
- В подобных системах используются проприетарные или специальные протоколы.

Отличия этих сред создают такие проблемы, как недостаточный уровень шифрования и аутентификации, слабые механизмы хранения паролей — все эти уязвимости могут быть использованы хакерами при захвате управления системами. Поскольку большинство сетей SCADA/ISC имеют определенную периферийную защиту, включая сегментацию сетей и межсетевые экраны, злоумышленники всегда ищут альтернативные пути для проникновения — например, через незакрытый шлюз или при помощи запуска определенных операций в организации, которые открывают канал передачи данных для внешнего проникновения. Среди типичных тактик:

- Использование портов удаленного доступа, предназначенных для обслуживания со стороны вендора;
- Взлом легитимного канала связи между ИТ-системами и ICS/SCADA;
- Принуждение путем обмана пользователя перейти по ссылке в письме на той рабочей станции, которая подключена как к сети ICS/SCADA и к Интернету (фишинговая атака);
- Заражение ноутбуков и/или съемных носителей за пределами сетей ICS/SCADA с целью дальнейшего вторжения во внутренние системы, когда они подключаются к сетям для сбора данных, обновления ПО контроллеров или сенсоров;
- Использование ошибок в конфигурации параметров безопасности.

Как только хакер проникает в сеть SCADA, он получает возможность запускать вредоносные команды на устройствах, вызывая сбой или задержку действий, связанных с соответствующими критически важными процессами, например открытия и закрытия клапанов.

В Казахстане как и во многих развитых странах, широко используются распределенные системы управления SCADA, т.к. в нашей стране быстро развивается нефте-

и газо-добыча/ переработка. SCADA-системы нашли широкое применение не только на рынке нефти и газа, а также и в передачи и распределения электроэнергии, альтернативной энергетики, воды и отработанной воды.Поэтому одна из поставленных задач перед специалистами - это безопасность SCADA-систем и создание эффективных, безопасных и выгодных SCADA-решений для своих пользователей.

Чтобы достичь нужного уровня защиты для промышленных и критически важных сетей, необходимо перейти от использования набора отдельных технологий и практик к эффективным бизнес-процессам. Эффективная стратегия безопасности должна обеспечивать обнаружение нетипичной активности и предотвращать атаки, одновременно предоставляя организации достаточную экспертизу для расследования взломов, когда они происходят.

Стратегия безопасности должна обеспечивать протоколирование всех активностей на отдельном уровне, не связанном с конфигурацией самих устройств SCADA, так как они могут быть взломаны при вторжении. Такой подход должен сопровождаться выработкой принципов допустимого поведения устройств SCADA с четким определением, что допустимо, что недопустимо и что следует считать подозрительным. Кроме этих мер стратегия должна включить автоматические уведомления и предотвращение отклонений от принципов, что позволит применять более эффективные меры против нежелательных активностей.

В дополнение к внедрению стратегии важно, чтобы вся ИТ-сеть организации была обеспечена средствами защиты для обеспечения безопасности устройств SCADA. Примеры взломов доказывают, что ИТ-среды, напрямую подключенные к Интернету, могут быть именно тем каналом, который обеспечит связь с технологическими операционными средами. Таким образом, важно реализовать механизмы, обеспечивающие только авторизованный доступ, контроль над приложениями и уведомления об идентификации, а также внедрить средства борьбы с угрозами — межсетевые экраны, системы предотвращения вторжений, антивирусы и системы эмуляции угроз.

Ключевым компонентом многоуровневой защиты для устройств SCADA должны быть средства интеллектуального анализа угроз (Threat Intelligence), чтобы передавать и собирать информацию о новых и развивающихся угрозах для критических инфраструктур. Внедряя технологии Threat Intelligence, организации могут защитить свои сети от киберугроз еще до того, как они проникнут внутрь. Это позволит обеспечить лучшую безопасность устройств SCADA и сделать их менее уязвимыми.

Киберугрозы, ориентированные на системы SCADA, получили значительное развитие за последние годы, и эта тенденция вряд ли изменится в ближайшем будущем. Хакеры становятся все умнее и все больше интересуются атаками на критические важные инфраструктуры. Поскольку уязвимости SCADA хорошо известны, эти сети находятся в зоне особого риска. Именно поэтому нужно внедрять новые стратегии и системы, которые помогут защитить сети и устройства и обеспечить безопасность не только отдельных организаций, но и общества в целом [4].

Список использованных источников

1. S. Rinaldi, J. Peerenboom, and T. Kelly, identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies". IEEE Control Systems Magazine, IEEE, December 2001, pp. 11-25.

2. Ensuring Reliable Production in a Dangerous Cyber World

3. Making Cyber Security Work in the Refinery

4. Ten, C.-W., Liu, C.-C., Manimaran, G.: Vulnerability Assessment of Cybersecurity for SCADA Systems. IEEE Transactions on Power Systems 23(4), 1836–1846 (2008)

(eds.) FPS 2012. LNCS, vol. 7743, pp. 357–364. Springer, Heidelberg (2013)