Как защитить коммунальные компании от угрозы вирусных атак

Во многих промышленных сетевых инфраструктурах, обеспечивающих обслуживание коммунальных систем, используются комплексные автоматизированные системы диспетчерского управления (Supervisory Control And Data Acquisition – SCADA) и системы распределенного управления (Distributed Control Systems – DCS) для автоматизации, мониторинга и управления важнейшими технологическими процессами. Важная роль и распространенность таких систем делает их наиболее вероятными мишенями для участившихся в последнее время вирусных атак криминальных и террористических организаций, преследующих цели приостановки их работы или вовсе разрушения всей инфраструктуры. Очевидно, что сбои в работе коммунальных компаний могут привести не только к прекращению оказания услуг, но и могут подорвать общественную безопасность.

Подобного рода атаки, предпринимаемые не с целью хищения данных, а для их безвозвратного удаления, используются правительственными органами и группировками активистов, которые при помощи вирусов проникают в локальные вычислительные сети и устраивают диверсии в различных отраслях, преследуя политические цели. Новая форма атак ставит под угрозу все коммунальные предприятия, оставляя их беззащитными.

Чтобы защитить коммунальную инфраструктуру от подобных атак, компания Dell SonicWall – дочерняя компания корпорации Dell, специализирующаяся на программных продуктах для компьютерной безопасности и защиты информации, рекомендует разработать четкую стратегию безопасности и предлагает положить в ее основу следующие десять шагов:

1. Изучите ваши системы SCADA. Изучите требования вашей системы SCADA к сетевой инфраструктуре, компонентам, приложениям, хранилищам и соединениям. Определите возможные внештатные ситуации и разработайте инструкцию по безопасной эксплуатации систем. Определите обязанности, права доступа и степень ответственности ИТ-специалистов, сотрудников и руководителей, а также других лиц.

2. Изолируйте ваш периметр. Отключите все ненужные и несанкционированные подключения к вашей SCADA-системе, в том числе незащищенные жесткие диски, USB-соединения, беспроводные соединения и соединения с другими внешними сетями (включая сети поставщиков, заказчиков, аутсорсеров и т. д.). Установите брандмауэр.

3. Укрепите оборону. Установите решения защиты, такие как системы унифицированного управления угрозами (Unified Threat Management – UTM) и брандмауэры нового поколения, которые помогут предотвратить возникновение отказов в критических узлах. Современные эффективные решения предлагают многостороннюю защиту, включая защиту от вторжений и вредоносного ПО, фильтрацию контента и управление сетевыми подключениями приложений.

4. Ограничьте доступ. Злоумышленники не смогут повредить системы SCADA и получить контроль над ними, если они не смогут до них добраться. Для этого требуется сформулировать и внедрить правила обмена данными и контроля доступа к информации, приложениям и ресурсам. Необходимо также выполнять постоянный мониторинг внешних соединений, которыми пользуются бизнес-пользователи, сотрудники обслуживающих организаций и т. д.

Определите уровень доступа на основе политик, ограничьте все привилегии доступа до необходимого минимума. Храните актуальный список учетных записей, регулярно проверяйте журналы и обновляйте все параметры доступа, где это целесообразно.

5. Обеспечьте защиту удаленного доступа. Появление большого количества мобильных устройств и беспроводных сетей повышает вероятность несанкционированного доступа. Обеспечьте защищенный удаленный доступ по сетям VPN, используя такие технологии защиты, как SSL.

6. Отключите ненужные функции SCADA. Некоторые функции SCADA (например, удаленное обслуживание) могут вести к снижению уровня защиты, так как предоставляют злоумышленникам дополнительный способ получения несанкционированного доступа и проникно-

вения в систему. Обратитесь к поставщику вашей SCADA-системы, чтобы узнать о возможности отключения функций без нарушения соглашений на обслуживание и возникновения перерывов в работе.

7. Следите за происшествиями и регистрируйте их. Пользуйтесь функциями мониторинга и журналирования во всех критических приложениях SCADA, инфраструктурах и т. д. Регистрируя происшествия и получая предупреждения о состоянии систем, вы сможете заранее предпринимать меры для отражения атак и поддержания непрерывного функционирования. Современные решения способны отображать весь сетевой трафик (включая приложения SCADA) в режиме реального времени и позволяют оперативно реагировать на непредвиденные ситуации.

8. Контролируйте внесение изменений и управляйте настройками. Сетевые настройки, системы, брандмауэры, доступ, приложения и процедуры могут меняться со временем. При этом, любое изменение может влиять на другие компоненты и соединения. Поэтому при внесении изменений в конфигурацию ведите журнал изменений и создавайте точки восстановления для того, чтобы избежать простоев в случае перезапуска. Существуют приложения для контроля самых сложных сетевых инфраструктур.

9. Проводите регулярные проверки. Проводите полные проверки систем каждые 6-12 месяцев. Регулярно проверяйте журнал происшествий, чтобы контролировать эффективность защиты (брандмауэров, сетевых компонентов и систем), соблюдение правил, правильность выполнения процедур и соблюдение прав доступа. Регулярно анализируйте результаты проверок и используйте полученные данные для корректировки и улучшения безопасности ваших систем.

10. Подготовьтесь к восстановлению. Являясь наиболее вероятной целью для вредоносных атак, SCADA-системы должны содержать резервные копии данных, чтобы в случае необходимости их можно было быстро восстановить. Позаботьтесь о разработке плана действий в чрезвычайной ситуации, чтобы обеспечить непрерывную работу вашего бизнеса. В число современных решений входят решения для автоматизированного создания резервных копий, обеспечения непрерывной защиты данных и восстановления на альтернативное аппаратное обеспечение.

Флориан Малеки (Florian Malecki),
директор по маркетингу продуктового направления в регионе EMEA,
компания Dell SonicWALL

НОВОСТИ

Инновационные решения Dell в рамках стратегии Connected Security

В октябре компания Dell во время ежегодного мероприятия Dell Technology Camp 2013, которое прошло в Париже, объявила о выпуске четырех новых продуктов в рамках стратегии безопасности Connected Security. Новинки созданы в ответ на вызовы сегодняшнего дня в таких актуальных технологических сферах, как BYOD, облачные вычисления, сетевая безопасность и соответствие стандартам. Комплексный всесторонний подход Dell, охватывающий все – от пользовательских устройств до центров обработки данных и "облаков", направлен на решение наиболее сложных проблем в сфере безопасности и соответствия отраслевым стандартам.

Решения Dell One Identity Cloud Access Manager, Dell ChangeAuditor 6.0, Dell InTrust 10.7 и брандмауэр нового поколения Dell SonicWALL NSA 2600 обеспечивают новый уровень защиты и предоставляют организациям возможность совместного сбора и анализа информации, а также возможность предпринимать упреждающие меры для защиты от угроз информационной безопасности.

Современные тенденции на рынке ИТ заставляют организации изменять подход к защите данных: сфокусироваться на защите соединений вместо того, чтобы организовывать закрытые изолированные хранилища. Для защиты данных, где бы они ни находились – в сети, "облаке" или на мобильном устройстве, – Dell предлагает воспользоваться подходом Connected Security, предлагая механизмы проактивного контекстного анализа. Кроме того, компания оказывает услуги по управлению безопасностью в комплексе с решениями SecureWorks, Dell Data Protection and Encryption.

Решение ***One Identity Cloud Access Manager*** предлагает функции управления локальными или облачными приложениями с помощью web-панели. А также:

- позволяет управлять доступом к локальным и облачным приложениям с различных устройств, включая настольные ПК, ноутбуки и мобильные устройства;
- предлагает дополнительный уровень защиты при использовании локальных и облачных приложений, таких как Salesforce, Google Apps и Office 365;
- предоставляет доступ с помощью web-браузера, используя универсальные параметры аутентификации, обеспечивает своевременное выделение облачных ресурсов, интеграцию, авторизацию и аудит.

НОВОСТИ

Устройство для сетевой безопасности ***SonicWALL Network Security Appliance (NSA) 2600*** оснащено запатентованной технологией Dell Reassembly-Free Deep Packet Inspection и использует более миллиона подключенных к Интернету источников данных. Это предоставляет организациям возможность блокировать новейшие угрозы сразу же после их появления, а также:

• позволяет предотвращать вторжения благодаря специальной технологии; удалять вредоносное программное обеспечение из сети с помощью простых инструментов; расшифровывать и проверять SSL-соединения; фильтровать контент/URL; выполнять наблюдение и контроль приложений и управлять сетевыми соединениями приложений;

• обеспечивает защищенный мобильный доступ на основе SSL VPN с устройств под управлением различных операционных систем, включая Windows, Linux, MacOS, iOS, Windows 8.1 RT и Android. Позволяет организациям внедрять многоуровневую защиту и контроль доступа как часть многоуровневой концепции BYOD;

• обеспечивает необходимый уровень защиты без ущерба производительности;

• содержит исчерпывающий набор простых в использовании функций, важных для компаний среднего и малого бизнеса. Эти функции помогают решать проблемы, связанные с WAN-подключением, балансировкой загрузки и безопасностью беспроводных сетей (при помощи интегрированного беспроводного контроллера).

Решение ***ChangeAuditor 6.0*** отслеживает и уведомляет в режиме реального времени об изменениях в конфигурации, изменениях, вносимых пользователями и администраторами. А также:

• позволяет просматривать, соотносить и фильтровать события и устанавливать связи между событиями по времени и в хронологическом порядке в среде Windows. Это позволяет лучше понимать события и тенденции и анализировать их;

• устраняет неизвестные проблемы и обеспечивает непрерывный аудит критически важных активов путем предоставления детализированной и стандартизированной информации об изменениях и связанных событиях по одному клику;

• реализует стратегию Connected Security путем обнаружения угроз и подозрительной активности, обеспечивая мгновенную реакцию с любого устройства в режиме реального времени.

Решение ***InTrust 10.7*** помогает организациям выполнять требования регулирующих органов и соответствовать внутренней политике безопасности за счет сбора, архивирования и поиска журналов регистрации событий в режиме реального времени. А также;

• обеспечивает слежение за доступом пользователей к критически важным системам и приложениям, анализ пользовательской и системной активности на основе истории событий;

• обеспечивает сбор событий об активности пользователей и администраторов с различных систем и приложений и представление данных в удобной форме для хранения и анализа;

• дополняет решения Dell SecureWorks интеллектуальными потоками данных, содержащих важную информацию о пользовательской активности на системах под управлением ОС Windows, помогает находить внутренние угрозы за меньшее время и при меньших затратах;

• реализует стратегию Connected Security, позволяя отойти от изолированных хранилищ и безопасно соединять информацию, пользователей, сети, приложения и услуги.

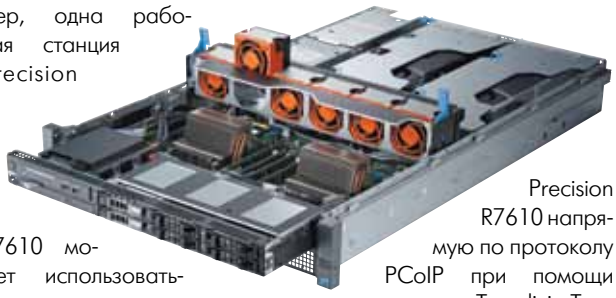
"Все наиболее яркие современные тенденции – "облака", BYOD/мобильность и Большие данные – несут целый ряд новых угроз. В результате организации сталкиваются с недостаточной эффективностью существующих моделей обеспечения безопасности и отсутствием необходимых ресурсов. В этом случае единственно верным выбором будет использование проактивных контекстных механизмов защиты. Они позволяют защищать данные в любом месте, где бы они ни находились. В рамках стратегии Connected Security компания Dell постоянно расширяет свой портфель предложений для решения наиболее сложных проблем в сфере безопасности и соответствия отраслевым стандартам", – сказал Мэтт Медейрос (Matt Medeiros), вице-президент и генеральный директор направления Security Products, подразделение Dell Software.

Рабочая станция Dell с поддержкой виртуализации

В последнее время появляется все больше новых приложений, которые позволяют быстро обрабатывать большие объемы данных. Это приложения для дизайнеров, инженеров и архитекторов, художников-мультипликаторов, ученых, исследователей и аналитиков.

Сегодня также растут требования к безопасности, в том числе и за счет того, что изменилась сама модель использования информации, когда средствами обработки (за счет их виртуализации) могут воспользоваться сразу несколько человек, находящихся в удаленных регионах в разное время суток. Централизованное размещение вычислительных мощностей в дата-центре позволяет повысить их управляемость и безопасность (что особенно критично при работе с конфиденциальной информацией), а также гибкость в предоставлении вычислительных ресурсов пользователям.

Рабочая станция Precision R7610 спроектирована в корпусе высотой 2U для монтажа в стойку. Эта модель оснащена возможностями дистанционного доступа, а ее функционал ориентирован на задачи виртуализации. Так, например, одна рабочая станция Precision R7610 может использоваться четырьмя сотрудниками для работы со сложными 3D-сборками путем проброса GPU в виртуальные машины и сертификации Citrix XenServer 6.1.0 с использованием функции Citrix XenDesktop HDX 3D Pro. Также пользователи могут подключиться к



Precision R7610 напрямую по протоколу PCoIP при помощи процессора Teradici Tera с нулевого клиента Dell Wyse P25 или Dell Wyse P45.

Подробности на сайте http://www.dell.com/ru/business/p/precision-r7610/pd.

Новый взгляд на офисные ИТ. PowerEdge VRTX.

Первое и единственное решение для полной интеграции серверов, систем хранения данных, сетевого оборудования и систем управления в форм-факторе 5U.

До сих пор не было ИТ-решения, созданного специально для офисных сред. Познакомьтесь с новинкой Dell PowerEdge VRTX на базе процессоров Intel® Xeon® – интегрированным комплексным решением, созданным специально для расширяющихся офисов. Это единственная платформа на базе общей инфраструктуры PowerEdge с форм-фактором 5U, созданная с учетом отзывов более чем 7 000 заказчиков и включающая четыре встроенных сервера, 48 Тбайт для хранения данных, сетевое оборудование и средства управления системами для упрощения всех аспектов ИТ-инфраструктуры. Вы вдохновили нас на это. Мы создали это.

Для того чтобы взглянуть по-новому на офисные ИТ, посетите страницу **Dell.ru/vrtx.**

Все, что вы хотели знать о VRTX и даже больше на Dell Solutions Forum 17 октября 2013 года в Москве: **DellSolutionsForum.ru**

The power to do more