Безопасность CAD/CAM/PLM-систем

Еще 100 лет назад в романах Конан Дойла Шерлок Холмс и доктор Ватсон расследовали кражу секретных чертежей из адмиралтейства Великобритании. С тех пор ситуация мало изменилась – конструкторская документация на современные продукты авиационной, аэрокосмической, автомобильной, судостроительной и иных отраслей является притягательной целью для многих промышленных шпионов и просто конкурентов. Изменились только форма хранения и разработки этих документов. Если раньше они создавались с помощью карандаша и ластика на чертежной доске, а сами документы хранились в бумажных архивах, то в эру высоких технологий для этого используются компьютеры, специальные системы автоматизированного проектирования (САПР) и системы управления жизненным циклом продуктов (Product Lifecycle Management, PLM). Об их безопасности – речь в настоящей статье.

Переход к электронным методам обработки, хранения и передачи технической документации повлек за собой явные прорехи в обеспечении защиты информации. Если украсть бумажные чертежи было не так просто – все-таки незаметно вынести из охраняемых помещений несколько листов формата A0 – не такая простая задача, то утащить сотни мегабайт данных на миниатюрной флэшке не составляет большого труда. А с учетом распределенности современных PLM-систем, которые базируются на IP-технологиях, используют широкий спектр взаимодействия, в том числе и на базе Web-сервисов, интегрируются с CRM-, ERP-, SCM-системами и т.п., степень уязвимости корпоративной информации многократно возрастает.

Информация, хранящаяся в PLM-системе, является критически важным для бизнеса ресурсом, так как содержит ноу-хау и другие промышленные секреты, позволяет дифференцироваться от конкурентов и, самое главное, позволяет быть конкурентоспособным и зарабатывать "на хлеб с маслом". Ни у кого нет сомнений в том, что PLM-системы и хранящаяся в них информация должны быть защищены от любых посягательств.

Однако если попробовать в системе поиска Google ввести ключевую фразу "CAD security", то, кроме 3D-элементов для САПР, вы ничего не увидите (в Рунете поиск также не дает результатов). Даже на сайтах самих производителей PLM-систем найти упоминания о мерах защиты непросто. Если такие меры и упоминаются, то, как правило, внимание уделяется таким вопросам, как аутентификация пользователей, обновление компонентов системы и регулярное резервирование информации. Ни о каком комплексном подходе не идет и речи. Более того, складывается впечатление, что производители даже не думали о возможности несанкционированного доступа к электронным чертежам и другой аналогичной информации.

Отношение разработчиков к вопросам безопасности своих продуктов ярко иллюстрирует пример компании SDRC (позже слившейся с UGS). Эксперты обнаружили "дыру" в архитектуре ее решения, через которую любой пользователь из любого места мог получить доступ к ядру системы с правами администратора. SDRC проигнорировала это сообщение и не предприняла никаких мер для устранения обнаруженной уязвимости. По счастью, злоумышленники не воспользовались этой возможностью, но привести она могла к весьма печальным последствиям. Гораздо меньше повезло в этом отношении американской аэрокосмической корпорации Lockheed Martin, у которой в 1997 году была совершена кража электронных чертежей и информации о конструкции самолета-невидимки Stealth. Обвинен в этом был российский хакер.

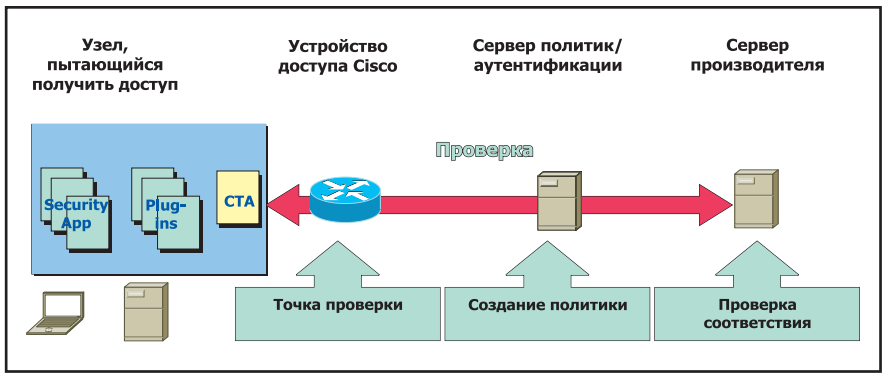
К основным угрозам при работе с PLM-продуктами можно отнести утечку конфиденциальной информации и нарушение работоспособности системы. Причем последняя угроза может быть реализована как с помощью атак, рассчитанных на отказ в обслуживании и выводящих из строя отдельные элементы CAD-систем, так и с помощью вирусов и червей, заражающих САПР. Так, еще в 2000 году был обнаружен первый вирус ACAD.Star для AutoCAD. Следствием таких неприятностей может служить уголовная или административная ответственность, финансовые претензии за упущенную выгоду или срыв договорных обязательств и, конечно же, недополучение собственной прибыли.

Какие меры позволяют защитить САПР? Мы выделяем 9 таких необходимых мероприятий.

1. ***Анализ рисков***. Прежде всего, необходимо определить, что является наиболее ценной информацией для организации, где она хранится и каков может быть ущерб от ее утери или утечки. Без ответа на эти вопросы невозможно определить целесообразность и эффективность всех остальных шагов.
2. ***Идентификация каналов реализации потенциальных угроз***. Зная достоверно, как в организации хранится, обрабатывается и передается информация, можно поставить надежную защиту на все потенциальные каналы реализации угрозы ее безопасности.
3. ***Отключение неиспользуемых функций***. Современные техно-

логии разрабатываются с прицелом "на будущее" и содержат большое количество функций, которые не востребованы многими заказчиками. Будучи активизированными, они могут служить точкой проникновения в PLM-систему. Поэтому все, что не требуется для работы, должно быть отключено.

4. ***Обучение персонала***. Поскольку сотрудники, работающие с CAD-системой, не являются специалистами по безопасности, их, так же как и всех сотрудников, имеющих отношение к работе с вычислительной техникой, необходимо обучить основам защиты информации.
5. ***Определение ответственности***. Очевидно, что, если за соблюдение сотрудниками правил безопасности никто персонально не отвечает, то и в нанесении ущерба винить тоже некого, а следовательно, наличие должного уровня информационной безопасности в такой организации находится под большим вопросом.
6. ***Разработка политики безопасности***. Мероприятия по защите САПР являются частью политики безопасности всех информационных ресурсов, а та, в свою очередь, частью концепции безопасности компании (не только информационной, но и физической, экономической и т.д.). Каждая организация должна иметь соответствующий документ (или набор документов), который в сжатой форме содержит описание всех процессов, связанных с обеспечением безопасности, перечень ответственных лиц, рисков и т.д. Именно на основе этого документа должна строиться вся работа организации.
7. ***Использование встроенных механизмов защиты программного обеспечения***.
8. ***Использование процедур расширенной безопасности***.
9. ***Регулярный аудит***. Какие бы меры защиты ни были внедрены, с течением времени они могут утратить свою эффективность, да и сами информационные потоки могут претерпевать

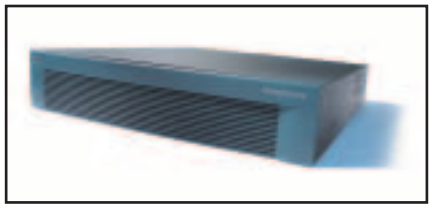


Cisco Network Admission Control

изменения. Поэтому необходимо регулярно проводить анализ того, что "есть", и отслеживать, как это соотносится с тем, как "должно быть".

Если говорить о технических мерах (пункты 7 и 8), то их можно разделить на 4 категории:

- отсечение "чужих",
- всесторонний контроль "своих",
- шифрование информации при передаче по сети,
- управление безопасностью и расследование инцидентов.



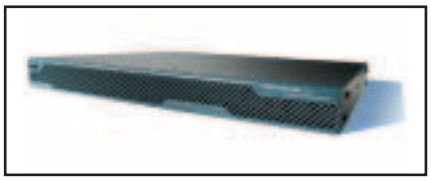
Cisco PIX 525 Firewall

Разграничение доступа позволяет реализовать принцип "минимума привилегий" и допускать к работе с САПР только авторизованных пользователей. При этом даже пользователей, имеющих право доступа, можно разделить по группам, чтобы иметь возможность сегментировать всю PLM-инфраструктуру в соответствии с различными требованиями по безопасности к каждой из групп. Реализовать данную задачу можно с помощью межсетевых экранов (firewall) и систем аутентификации. Причем аутентифицировать можно не только самих пользователей, но и компьютеры, с которых они подключаются к САПР. Можно пойти еще дальше и проверять, насколько конкретный компьютер соответствует политике безопасности – имеются ли на нем актуальные антивирусные программы, настроена ли система защиты, установлены ли все необходимые патчи и т.д. Это позволит гарантировать, что даже авторизованный, но нерасторопный пользователь, забывший вовремя обновить свой антивирус, не станет причиной снижения уровня защищенности корпоративных ресурсов. Такая технология получила название Network Access Control, называемая некоторыми производителями также Network Admission Control или Network Access Protection.

Однако разграничение доступа еще не решает всех проблем с безопасностью. Необходимо также контролировать защищенность рабочих станций и серверов, на которых функционирует САПР. Это делается с помощью систем предотвращения атак уровня узла (HIPS). Они не только контролируют поведение пользователей и приложений, но и блокируют любые попытки нарушения политики безопасности. Дополнением систем данного класса являются средства контроля утечки информации через периферийные носители – USB, PCMCIA, CD, COM-порты, дискеты и т.д.

Учитывая, что современные PLM-системы работают в распределенном режиме, необходимо решить еще две задачи:

- защитить передаваемый между компонентами трафик. С этой целью применяются технологии построения виртуальных частных сетей (VPN). Главное, о чем надо помнить в данном случае, – это о соответствии законодательству. В России есть определенные требования к системам шифрования, невыполнение которых может повлечь за собой определенные административные последствия;
- обеспечить предотвращение атак, направленных на компонен-



Cisco IPS 4255 Sensor

ты САПР. Системы, выполняющие эту функцию, носят название сетевых систем отражения атак (IPS).

При выборе технических мер защиты необходимо помнить, что они могут быть как интегрированными в инфраструктуру, так и реализованными в виде отдельных программных или программно-аппаратных решений. Интеграция позволяет сделать защиту более эффективной (за счет тесного взаимодействия с инфраструктурой) и снизить размер инвестиций.

Важно понимать, что единой технологии обеспечения безопасности не существует, но на настоящий момент разработана многоуровневая стратегия, в соответствии с которой выполняется интеграция компонентов безопасности во все устройства. Следование этой стратегии позволяет обеспечить наиболее эффективную защиту даже небольших САПР, не говоря уже о территориально-распределенных внедрениях.

К сожалению, производители PLM-продуктов не уделяют должного внимания вопросам безопасности их использования, что не позволяет задействовать встроенные возможности самих систем. Однако при правильном применении "внешних" защитных механизмов и мер, описанных выше, можно построить действительно защищенную систему управления жизненным циклом продукта и не беспокоиться ни об утечке информации, ни о нарушении работоспособности компонентов САПР. При этом основные этапы построения системы безопасности не требуют серьезных денежных затрат и усилий. А результат – гарантия выпуска продукции в срок и возможность обойти конкурентов "на вираже".

А. В. Лукацкий,
бизнес-консультант по безопасности,
компания Cisco Systems

СОБЫТИЯ

CiscoExpo 2006 в Москве – седьмая, рекордная

Ежегодная конференция CiscoExpo проводится во многих странах мира и имеет репутацию одного из самых крупных и авторитетных мероприятий в IT-индустрии. На этих форумах компания представляет общественности всестороннюю информацию о своих новейших технологических разработках и ближайшей стратегии развития. В столице России этот форум проводился уже в седьмой раз, но никогда еще он не вызывал к себе такой интерес пользователей и не пользовался столь широкой поддержкой лидеров IT-индустрии, а также специализированных и отраслевых средств массовой информации: в этом году в работе конференции приняло участие свыше 1600 человек.

Московская конференция, как и другие форумы CiscoExpo этого года, была посвящена стратегии развития защищенной интеллектуальной информационной сети (Intelligent Information Network, IIN). Согласно определению, данному старшим вице-президентом компании (Cisco Systems) Доном Проктором, выступившим на форуме с программным докладом, под интеллектуальной информационной сетью в компании понимается платформа, способствующая росту бизнеса коммерческой организации.

По сложившейся традиции особое внимание на CiscoExpo-2006 было уделено вопросам безопасности. При современном уровне развития информационных технологий обеспечение безопасности ведения бизнеса является одной из самых приоритетных задач. Открытие сетей для большего числа пользователей и приложений приводит к росту уязвимости информационных ресурсов, что, в свою очередь, делает еще более актуальной необходимость повышения уровня их защищенности от внешних и внутренних несанкционированных воздействий.

Исходя из интересов своих заказчиков и партнеров, Cisco Systems уделяет решению этой задачи исключительное внимание. На исследования и разработки в сфере информационной безопасности компания ежегодно расходует около 10 % всех ассигнований на НИОКР, или около 300 млн долларов в год. Такой подход позволяет Cisco Systems лидировать практически во всех сегментах рынка средств защиты информационных ресурсов.

Работа конференции проходила по пяти техническим потокам, в составе которых проводились сессии с углубленным изучением определенных тематик. Кроме того, были организованы сессии по технологиям и решениям компании Cisco Systems и спонсоров конференции.

По ряду тематик, активно обсуждаемых в IT-сообществе, на конференции прошли открытые дискуссии. Среди них, помимо вопросов обеспечения безопасности, решения по передаче, хранению и обработке голосовой и видеоинформации, центры обработки и сети хранения данных, маршрутизация и коммутация в корпоративных и провайдерских сетях. Участники дискуссий обсуждали новые решения по управлению сетями, новинки в вопросах построения оптических сетей и сетей Metro Ethernet, делились своими соображениями по технологическим решениям для центров обработки вызовов, а также новым сервисным услугам и программам Cisco Systems.

Помимо рабочих заседаний в рамках конференции прошла выставка продуктов и технологий компании Cisco Systems, спонсоров и партнеров CiscoExpo. Как самостоятельный элемент форума CiscoExpo выставка также получила поддержку рекордного числа компаний: одиннадцать международных и российских брендов приняли на себя официальный статус партнеров по ее организации.