Как защитить данные внутри локальной сети?

Рост интереса среди компаний к вопросам безопасности сетевого доступа нарастает на протяжении последних двух десятилетий. В течение этого времени непрерывно развиваются механизмы управления доступом – от первых широко распространенных каталогов до современных систем комплексной идентификации пользователей, групп и ролей в инфраструктуре предприятия, которые делают процесс предоставления доступа более простым и предсказуемым.

Можно понять хакера, который сломал защиту периметра сети, или "чрезмерно умного" пользователя, который перехватывает сетевой траффик, так как это спланированные "военные" действия на "рубежах" информационной безопасности. Но трудно найти оправдание ИТ-департаменту, допускающему несоблюдение пользователями политик безопасности, приводящих к нарушению параметров секретности и целостности данных. Решение данных вопросов целиком находится в рамках обязанностей ИТ-отдела, но большинство ИТ-руководителей не придают им должного значения.

Есть много вопросов, представляющих существенный риск для информационной безопасности, которые можно задать любой компании и на которые большинство организаций, скорее всего, не смогут ответить с уверенностью:

- Сколько у вас учетных записей, которые не использовались более 60 дней?
- Сколько у вас групп безопасности, которые являются дубликатами или не используются?
- Скольким пользователям разрешено не менять пароли?
- Сколько пользователей, у которых права на ресурсы заданы в явной форме, а не определены членством в группе?
- Кто имеет доступ к конфиденциальной финансовой или личной информации?
- Если конфиденциальная информация была перемещена, то куда именно она была перемещена? Кем была перемещена? И зачем?
- Открывал ли системный администратор файлы с конфиденциальной информацией? Если открывал, то когда?
- Существуют ли добавленные в группу администраторов пользователи, не имеющие данных полномочий?
- Если учетная запись была заблокирована в связи с неправильным вводом пароля, то это ошибка пользователя или злой умысел?

Помимо этих существует еще много подобных вопросов. Например, часть данных можно получить из журналов системных событий или в виде системных записей. Но большинство из этих записей или "сырые" (требуют дополнительного анализа) или не сохраняются в системе вовсе. Поэтому специалистам очень трудно определить то или иное событие с достаточной точностью.

К счастью, существуют рекомендации, которые дают представление о том, как следует управлять информационной безопасностью на предприятии, а также автоматизированные решения, позволяющие оценить и улучшить показатели в данной области. Лучшие мировые практики в области обеспечения информационной безопасности объединены в едином документе – ISO 27002, созданном Международной Организацией Стандартизации. Данный стандарт наиболее четко описывает процессы управления безопасностью доступа к сети. В соответствии с данным стандартом созданы автоматизированные решения по контролю доступа к сетевым ресурсам компании NetVision, имеющей более чем десятилетний опыт в этой области.

Какие существуют проблемы?

Важный момент, который нужно учитывать при обеспечении безопасного доступа к информации – это определение, какие ресурсы свободно доступны пользователям, а какие должны быть жестко контролируемы. Было бы идеально, если бы права на доступ к ресурсам устанавливались один раз и навсегда. Но на практике критерии безопасности доступа постоянно изменяются, что усложняет процесс защиты сетевых ресурсов. Например, параметры доступа к общим файлам или элементам почтовой системы, такие как MS Exchange, могут быть изменены непосредственно пользователями, минуя процесс управления изменениями, что добавляет сложностей в процесс управления доступом. Таким образом, основной задачей защиты сетевых ресурсов является назначение всем пользователям определенных прав доступа и постоянный контроль их изменений.

С другой стороны, доступ к бизнес-приложениям, работающим с конфиденциальной информацией, предоставляется ограниченному количеству сотрудников, изменяется редко и инструмент изменения прав доступа находится только у администраторов данных бизнес-систем. Это проблема иного характера, но она не менее важна, чем задача предоставления общего доступа к ресурсам.

Чтобы не выходить за рамки журнальной статьи, сфокусируем свое внимание на вопросах безопасности доступа к ресурсам в сети.

В повседневной работе, когда изменения исчисляются сотнями или даже тысячами в день, что бывает при большой децентрализации компании, организации должны быть уверены в том, что:

- пользователи, которые в данный момент имеют доступ к тому или иному ресурсу, на самом деле должны его иметь;
- пользователь получил этот доступ законным путем;
- пользователь правильно использует информацию, к которой у него есть доступ.

Как выбрать?

Первый принцип организации системы безопасности – это определение потенциально опасных мест. Без определения областей риска, без осуществления постоянного мониторинга и внедрения системы контроля невозможно надежное обеспечение информационной безопасности. В любой компании производится огромное количество всевозможных действий с информацией, и среди них трудно выделить несанкционированную деятельность. Здесь следует прежде всего ответить себе на следующие вопросы:

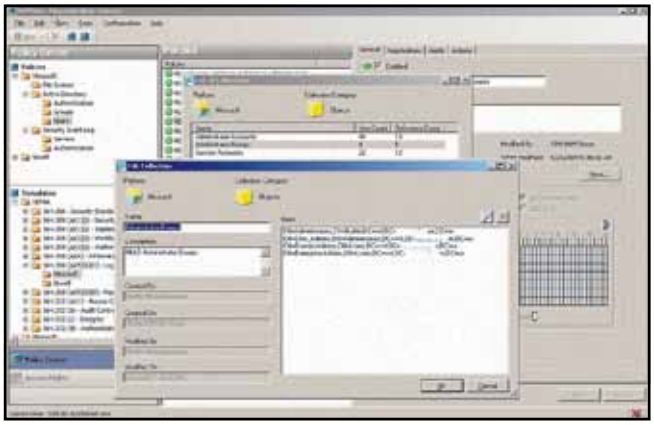
- Существуют ли в компании процессы по обеспечению безопасности? Например, процедура смены пароля или регулярный обзор прав доступа к ресурсам или блокировка доступа неактивным пользователям.
- Существуют ли пользователи или группы пользователей, к которым применяются более высокие требования безопасности или деятельность которых необходимо отслеживать? Это могут быть тестовые учетные записи, учетные записи администраторов или операторов критически важных бизнес-систем, содержащих конфиденциальную информацию.
- Определены ли типы активности, которые более критичны с точки зрения безопасности по сравнению с остальными действиями пользователя? Например, действия администраторов почтовых систем над почтовыми ящиками, чтение или модификация файлов, которые относятся к конфиденциальной или персональной информации.

Определены ли типы действий, которые можно однозначно характеризовать как потенциально опасные? Например, перенос файлов из папки общего доступа, отправка почтового сообщения от лица другого пользователя, добавление новых пользователей в группу.

Второй принципиальный момент – оценка состояния параметров доступа на текущий момент. Продукты NetVision NVAssess и Access Rights Inspector – это комплексное решение для данной задачи. В первую очередь они нужны для определения типов учетных записей, групп и других объектов, а также для установки уровня контроля над ними. Например, можно определить большое количество учетных записей, которые активны, но не использовались в течение 90 дней. Это может быть базой для создания политики безопасности, на основе которой будут отслеживаться неиспользованные учетные записи с их последующей блокировкой. Другой пример – определение учетных записей, находящихся на тестировании или имеющих расширенные права доступа, для их последующей группировки и применения к ним уникального шаблона мониторинга. Access Rights Inspector – программный продукт, который в процессе сканирования сети может предоставить такие данные, как список всех ресурсов, к которым имеет доступ определенный человек, или список группы, которая имеет доступ к данному ресурсу. Программа может собирать и выстраивать информацию как о наличии разрешений для групп пользователей, так и о параметрах безопасности сетевых ресурсов, помогая администраторам быстро находить потенциально уязвимые места.

Далее необходимо самостоятельно определить, какие типы изменений могут иметь потенциальные риски для безопасности и затем воспользоваться NetVision NVMonitor для создания правил мониторинга и сбора информации об изменениях на основе критериев, определенных на первых двух шагах.

Важной частью этого шага является составление требований к собираемым данным и определение уровня секретности для критериев мониторинга и хранилища данных. В ISO 27002 рекомендовано использовать защиту от несанкционированного доступа для всех собираемых в ходе мониторинга данных. Использование продуктов NetVision обеспечивает дополнительный уровень защиты, так как консоль управления, в которой задаются параметры безопасности, может быть ограничена по доступу и не включать разрешения для всех системных администраторов. При использовании консоли ведется также подробный журнал, а такой уровень конт-



Создание коллекции объектов мониторинга – Административные группы

Создание коллекции объектов мониторинга – Объекты слежения

роля не поддерживается стандартным системным функционалом. Некоторые клиенты NetVision идут дальше и перекладывают задачи по анализу собранных данных на системных интеграторов, а в самой организации доступ к журналам никто не имеет.

Четвертый шаг – это проведение расследования и принятие мер. В ISO 27002 это описано так: "инциденты должны быть зафиксированы, проанализированы, а для исправления должны быть произведены соответствующие действия". Именно на этом этапе NetVision предоставляет основное преимущество, поскольку заложенный в продукте функционал позволяет отследить и оповестить обо всех событиях, которые на основании созданных критериев являются подозрительными и требуют вмешательства. Таким образом, рекомендация "зарегистрировать, проанализировать и принять меры" сводится лишь к одному действию – "зарегистрировать".

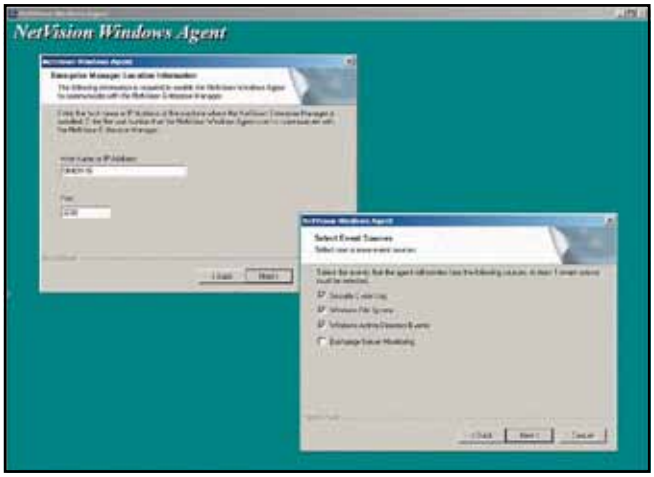
Итак, инструментарий, реализованный в продуктах NetVision, поможет специалистам больше своего времени отдавать работе по усилению безопасности сетевых ресурсов. К ней относятся чистка групп безопасности, изоляция или архивация устаревших данных, находящихся в общем доступе, удаление учетных записей после увольнения сотрудников или просто рутинная проверка правильности установки разрешений к ресурсам.

Как автоматизировать?

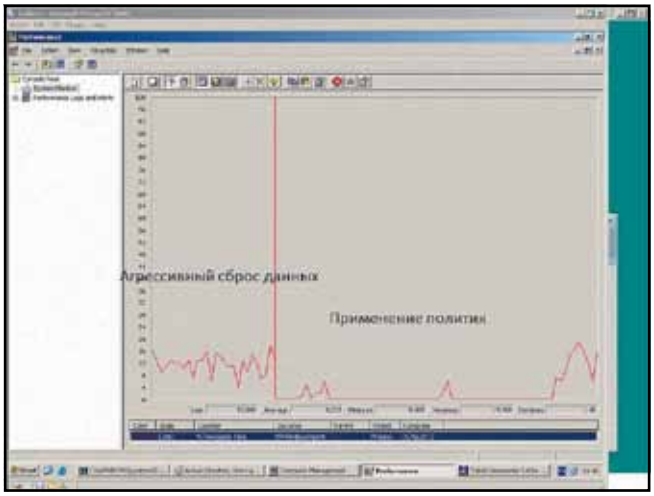
Существует много продуктов, которые предлагают автоматизировать процессы обеспечения безопасности. Приведем несколько полезных рекомендаций, которыми можно руководствоваться при выборе соответствующего решения.

Основная рекомендация – решение должно обеспечивать контроль информации, "не позволять данным управлять тобой". Как уже говорилось, если слишком много данных проходит через вас, то, скорее всего, будет очень сложно определить, какие из них важны для принятия правильного решения, а какие – нет. Поэтому мы рекомендуем, чтобы система автоматизации имела возможность предоставлять именно ту информацию, которая вам необходима в данный момент. Способность генерировать детализированные отчеты с широкими возможностями фильтрации позволяет не только получать необходимую информацию в полном объеме, но и снизить ее влияние на производительность системы в целом. NVMonitor является именно такими продуктом, с возможностью гибкой настройки шаблонов мониторинга под конкретные задачи.

Следующая рекомендация – оценивать продукты по их способности предоставлять данные, которые в дальнейшем можно будет использовать при расследовании инцидентов в сфере информационной безопасности из журналов событий системы или других уже существующих источников. Зачастую эти источники выглядят как список всех событий, происходящих в системе и выстроенных по дате создания. Например, вы помните, что означают события Microsoft Event ID, но большинство людей – вряд ли. Поэтому запись о том, что произошло событие ID 541, не очень информативно. Если вам нужно



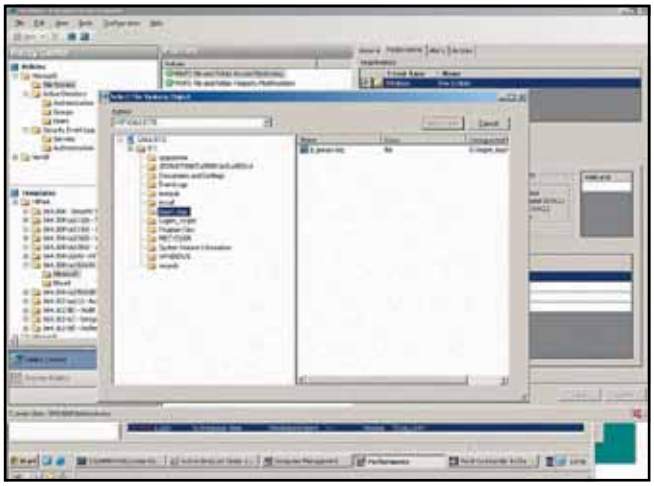
Установка Агента – минимум действий или автоматический режим



Работа Агента

проанализировать несколько записей, задача еще более усложняется. В продуктах NetVision основной упор сделан на представление информации, имеющей достаточную полноту для принятия необходимых решений.

В некоторых случаях часть параметров объектов системы нигде не сохраняется, что усложняет процесс отслеживания изменений. Решения NetVision тесно интегрированы в операционную систему с целью получения данных, которые в дальнейшем будут использованы для оценки событий.



Политика мониторинга файловых ресурсов – выбор объекта

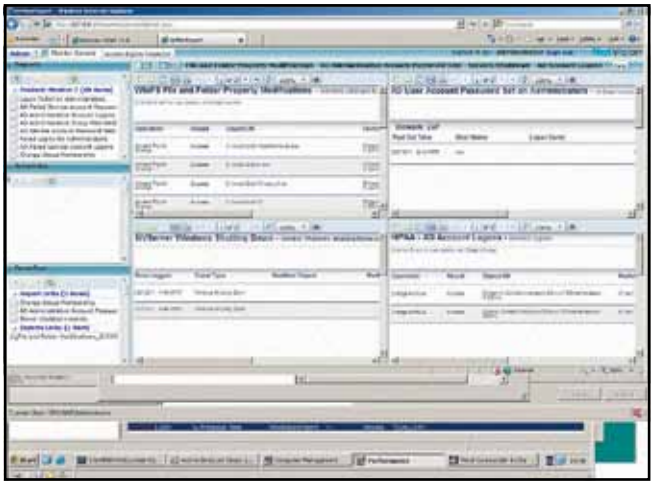
Продукты NetVision позволяют также создавать одинаковые отчеты, как для разных доменов, так и для разных групп администраторов. То есть, мы еще раз возвращаемся к тому, что информация должна предоставляться для каждого специалиста именно в том объеме, который ему необходим, не больше, но и не меньше.

Последняя рекомендация – в выбранном решении должна быть предусмотрена автоматизация корректирующих действий. Так, продукты NetVision могут автоматически выполнять действия при возникновении того или иного события. Например, обнаружив, что у вас есть 10 учетных записей, которые не использовались в течение 120 дней, система может их автоматически отключить. Это очень удобно, но нужно быть очень аккуратным в реализации данной функции. Блокируя событие, вы никогда не узнаете о том, что на самом деле была попытка предпринять злоумышленные действия. Пусть лучше событие произойдет и его можно будет зафиксировать, изучить, а в дальнейшем предотвращать. Специалисты организации должны определиться, будет ли приобретаемый продукт использоваться в качестве инструмента анализа состояния безопасности доступа или в качестве автоматизированной системы процесса управления доступом.

Как избежать проблем?

Все проблемы, возникающие вследствие отсутствия обдуманного, комплексного подхода к процессу обеспечения безопасности доступа к общим ресурсам, примерно похожи. Основной мотив, который побуждает ИТ-департамент автоматизировать управление процессом доступа, – это стремление максимально снизить затраты, связанные с проведением рутинных изменений, а не обеспечение безопасности как таковой. С другой стороны, администраторы часто тратят очень много своего времени, чтобы понять первопричину возникновения крупных инцидентов. Например, нередко бывает так, что пользователь случайным движением мышки перенес папку с документами на общем ресурсе в другое место, соответственно другие пользователи этих данных не увидят, что вызовет огромный шквал звонков в службу поддержки. А работники службы поддержки в свою очередь будут "атаковать" администраторов, которым потребуется время, чтобы понять, что произошло. Часто наблюдается и такая ситуация, когда один администратор тратит продолжительное время на проведение изменений в системе, которую до него настраивал другой администратор, так как он не владеет информацией о том, что было сделано ранее. Подобные ситуации могут показаться малозначительными, если бы не частота, с которой они возникают в разных организациях, и не серьезные затраты времени у заказчиков, уходящие на то, чтобы собрать все изменения воедино и произвести коррекционные действия. Многие компании также жалуются на ситуацию, когда им приходится тратить часы на воспроизведение прав доступа в случае консолидации ресурсов общего пользования или переноса данных с сервера на сервер.

Практически каждый администратор подтверждает, что в течение срока эксплуатации информационных систем на предприятии скапливается большое количество несоответствующих действительности прав, которые должны быть



Отчеты – четыре отчета одновременно, комбинированный вид

Комбинированный отчет – диаграмма и список

удалены. В то же время администраторы понимают, что у них нет инструмента для анализа прав доступа, необходимого для дальнейшего редактирования данных.

Как реализовать преимущества?

Большинство организаций, внедривших у себя комплексные системы управления доступом, подтвердили возврат инвестиций в течение года. Это достигается за счет более рационального использования рабочего времени специалистов, которые вместо того чтобы тратить часы на исследование ситуации, обладая необходимой информацией, имеют возможность проведения коррекционных действий.

Очевидно, что в вопросах безопасности невозможно решать проблемы "точечно", так как это не даст положительных результатов. Решение должно быть только комплексным, а также отвечать требованиям стандарта ISO 27002. В этом случае вы получите защищенную сетевую инфраструктуру, дающую уверенность в том, что доступ предоставлен соответствующим образом и используется по назначению.

David Rowe, компания NetVision,
Александр Рыбинский, продукт-менеджер NetVision,
Максим Новиков, ведущий инженер,
Группа компаний ARBYTE