

«БМС Консалтинг»: внедрение комплекса централизованного управления и мониторинга информационной безопасности

Управлять средствами информационной безопасности в организации, где количество серверов и рабочих станций не превышает 30 единиц, — дело под силу одному-двум опытным администраторам. Но что делать в случае развитой инфраструктуры крупной организации? Как отслеживать состояние серверов, парк которых насчитывает более 100 единиц, разбросанных в разных отделениях и филиалах по разным регионам, и сервисов, предоставляемых этими серверами?

eTrust Security Command Center

В ходе недавнего проекта в качестве инструмента, способного решать подобные вопросы, компанией «БМС Консалтинг» было предложено решение CA eTrust Security Command Center, включающее сервер централизованного управления eTrust SCC, средство сбора и корреляции событий eTrust Audit и средство централизованного управления доступом пользователей eTrust Access Control.

Предложенное решение удовлетворяло всем требованиям клиента и учитывало особенности ИТ-инфраструктуры организации.

В первую очередь решался вопрос с гетерогенностью среды. Основные сервисы организации в равной степени функционируют как на серверных платформах семейства Windows, так и на Unix-системах. Компоненты-агенты системы eTrust Audit в полной мере обеспечивают сбор событий от неограниченного количества источников как Windows NT EventLog, так и Syslog Unix. Кроме этого, на вооружении eTrust Audit имеется полный спектр агентов для сбора событий от систем информационной безопасности, среди которых — вся линейка продуктов CA eTrust, ISS RealSecure, антивирус McAfee, и прикладных систем, таких как системы управления базами данных (Oracle, MS SQL), Web-серверы (Apache, IIS), прокси-серверы (Squid) и т.д.

Следующим требованием было обеспечение централизованного

и долгосрочного хранения событий аудита, а также возможность быстрой корреляции событий и предоставления информации как в оперативном режиме, так и в виде отчетов различной сложности. Сбор событий в eTrust Audit осуществляется в централизованном хранилище — коллекторе событий, в качестве его платформы может выступать СУБД Oracle или MS SQL. Кроме этого, существует возможность определения более одного коллектора, что дает возможность 100% сохранения события.

Для централизованного управления доступом и аудита прав пользователей было решено использовать средства eTrust Access Control. Благодаря гетерогенности системы, обеспечивается возможность управления доступом пользователей к ресурсам, предоставляемым как серверами Windows, так и серверами, работающими под управлением Unix. Кроме того, централизованное управление дало возможность выполнять аудит текущих прав пользователей, без необходимости анализа каждого сервера по отдельности.

Одним из главных требований заказчика являлось обеспечение интеграции системы централизованного управления и мониторинга информационной безопасности с

существующим специализированным ПО организации. eTrust SCC представляет гибкий API для интеграции приложений как со средствами аудита событий, так и с централизованным сервером управления. Предоставляемый SDK обеспечивает быстрое написание компонентов-агентов с использованием различных языков программирования (C++, Visual C, Java), тем самым дает возможность сбора событий из любых источников.

Преимущества внедрения

Главное преимущество — это гибкость решения: возможность функционирования на различных программных платформах, множественные средства сбора событий аудита, организация отдельных хранилищ событий для разных источников, проектирование индивидуальных «рабочих столов» пользователей — все это дает возможность построения универсального комплексного центра управления информационной безопасностью.

Кроме того, наличие открытого API позволяет выполнять интеграцию eTrust SCC с любыми системами, расширять функциональные возможности и распространять использование системы всеми подразделениями ИТ.

Использование широких возможностей визуализации объектов мониторинга позволяет построить иерархические представление данных о текущем состоянии ИТ-инфраструктуры организации в целом.

Использование ролевого администрирования позволяет реализовать модель разделения полномочий и ответственности между группами администраторов и менеджеров.

Таким образом, благодаря поддержке гетерогенной среды, гибкости настройки и наличию средств расширения функциональных возможностей, внедренное компанией «БМС Консалтинг» решение значительно облегчило жизнь всем сотрудникам ИТ в компании, выполняя за них огромный объем однотипной работы, способствовало повышению общего уровня информационной безопасности.

Кроме того, наличие системы управления и мониторинга является требованием многих международных стандартов в области ИТ, что актуально для компаний выходящих на международные рынки.

■ **Андрей Майба,**
консультант сектора
информационной
безопасности компании
«БМС Консалтинг»,
Andrey_Mayba@bms-
consulting.com

Сначала — кто, затем — что

В организациях с разветвленной инфраструктурой, где могут присутствовать различные гетерогенные сети, наиболее актуальным становится вопрос управляемости и совместимости. Но еще более насущным был, есть и будет вопрос информационной безопасности, управлению которой в организациях уделяется не так много времени, как хотелось бы.

Разносторонне исследуя эту проблему, мы пришли к выводу, что основным звеном в управлении информационной безопасностью является человек. В вопросе информационной безопасности вопрос компетентности сотрудника важен, если учесть, что согласно общемировой статистике 80% всех ургоз ложится на плечи сотрудников компании. В связи с этим хочется отметить, что подготовка специалистов должна стоять на первом месте, ведь от уровня подготовки и информированности каждого отдельно взятого сотрудника зависит, насколько компания сможет быть защищенной.

Подготовка специалистов зачастую требует комплексного подхода. Конечно, каждый специалист инди-

видуален как по уровню знаний, так и по функциональным обязанностям. Проведение индивидуальных занятий для каждого требует больших затрат. В связи с чем и появляются на рынке образования комплексные подходы к обучению специалистов.

Комплексная программа подготовки администраторов информационной безопасности — это шаг в сторону развития комплексного подхода, который сегодня делает Академия «БМС Консалтинг». Программа построена таким образом, чтобы на каждом этапе обучения можно было оценить, насколько усваивается материал слушателем и можно ли эффективно проходить следующий курс программы. Кроме этого, перед прохождением программы обучения слушателям предлагается пройти тестирование для проверки собственных знаний, что в некоторых случаях дает дополнительную информацию для осознанного выбора тематики обучения

■ **Алексей Машаров,** директор учебного центра «Академия БМС Консалтинг»,
Alexiy_Masharov@ec.bms-consulting.com