Мониторинг действий пользователей: презентация на международном семинаре Группы «ЛУКОЙЛ»

написано GlobalTrust.ru | 15.07.2012

Компания GlobalTrust приняла участие во втором международном семинаре «Обеспечение информационной безопасности Группы «ЛУКОЙЛ», который проводился в период с 8 по 15 июля в г. Сочи. Целью данного мероприятия является обмен опытом между заказчиками, консультантами и поставщиками решений по информационной безопасности, демонстрация новейших достижений в этой области.

В рамках семинара GlobalTrust представил специалистам Группы «ЛУКОЙЛ» наиболее продвинутые средства для мониторинга действий пользователей корпоративной сети.

Отрывок из выступления Александра Астахова (Генерального директора GlobalTrust) на семинаре:

«Понятие «информационная безопасность» для разных людей имеет разный смысл. Для простого обывателя это набор мифов и полуправды о компьютерных вирусах и всесильных хакерах. Для «айтишников» – это джентльменский набор из антивирусов, межсетевых экранов, VPN и средств обнаружения вторжений. Для менеджеров это, прежде всего, документы и процедуры, для бывших военных – это противодействие техническим разведкам и предотвращение утечки информации по техническим каналам.

Конечно для решения столь сложной задачи как обеспечение информационной безопасности необходимы различные специалисты и подходы. Однако есть одно фундаментальное условие без которого все эти подходы не приносят желаемого результата. Это то, что лежит в основе самого понятия информационной безопасности. Это контроль над использованием информации. А если еще конкретизировать, то это контроль над людьми использующими информацию, контроль всех их действий, всех

коммуникаций, всех контактов и даже их привычек и особенностей выполнения работы.

Чем занимаются службы безопасности (неважно какой) по всему миру? Прежде всего наблюдают за вероятным противником, скурпулезно фиксируют все его шаги и пытаются спрогнозировать возможные действия. Своих целей добивается тот, кто лучше осведомлен. Шахматисты в обязательном порядке записывают все ходы противника и тщательно их анализируют, а лучший способ защиты в шахматах, как известно, контратака.

Безопасность — это своего рода игра, в которой выигрывает тот, кто лучше осведомлен. Успех корпоративной информационной безопасности определяется прежде всего степенью контроля ситуации: кто чем занят? кто с чем или с кем работает? Что они собираются предпринять? Кто нарушает или пытается нарушить правила безопасности? Кто готовит для вас сюрприз? Сотрудники организации чувствуют, что безопасники должны это знать. Они подозревают в чем должен быть основной смысл нашей работы и это одна из причин настороженного отношения к безопасникам в любой организации. К сожалению, как показывает наша консалтинговая практика, сами сотрудники служб информационной безопасности часто об этом не подозревают. Они бывают сосредоточены либо на внедрении сложнейших программно-технических комплексов защиты информации, либо на разработке организационно-распорядительных документов, либо на бесконечных совещаниях и управляющих комитетах, и понятия не имеют о том, что происходит за рабочими местами пользователей и администраторов корпоративной сети. А это означает, что они не контролируют по крайней мере 70% существующих рисков информационной безопасности.

Обычно практикуется три вида мониторинга: трафика, логов, электронной почты. При этом используются сложнейшие сигнатурные, статистические, эвристические и лингвистические методы. Однако все эти меры направлены против внешних злоумышленников, чтобы по косвенным признакам обнаружить опасные действия. Нам же в первую очередь надо контролировать собственных пользователей и администраторов. Когда объектом мониторинга является корпоративная сеть мы имеем возможность контролировать все действия пользователей непосредственно на рабочих местах, что намного эффективнее».

astahov_spector360Скачать