Защита уязвимых данных с помощью аналитики поведения пользователя и организации (UEBA)

В современном мире неприятная действительность заключается в том, что кибератаки происходят. Недавние кибератаки на BlueShield, Калифорния и AMEX только доказали, что текущие подходы безопасности к обнаружению угрозы и реагирования на нее не позволяют защитить организации от передовых нападений. Организации сегодня должны быть в состоянии составить полную картину дорогостоящих IT-систем, профили пользователей и важных приложений, чтобы эффективно предсказывать и защищаться от этих видов угроз. В случае Blue Shield и AMEX нарушения можно было идентифицировать задолго до того, как стало слишком поздно.

В случае Blue Shield, злоумышленники проникали в корпоративную сеть в течение почти года перед тем, как были обнаружены. Нападавшие эксплуатировали уязвимость систем организации и нарушили доступ к ресурсам учетных записей пользователей. Нарушение данных AMEX демонстрирует, как киберпреступники крадут законные пользовательские учётные данные из организаций, чтобы достичь конечной цели – в данном случае данные кредитной карты.

Современные угрозы имеют сложный характер развития, связанный с миграцией точек проникновения по ресурсам организации. Чтобы гарантировать полностью безопасную информационную среду, каждая организация должна удостовериться, что у неё есть правильный набор инструментов безопасности для защиты конфиденциальной информации. Независимо от того, исходит ли угроза изнутри сети или снаружи, наличие правильного набора инструментов для обеспечения своевременного обнаружения угрозы и хорошо управляемой защиты для борьбы с этими угрозами, значительно уменьшает шанс на успех любого киберпреступника.

Применение передовой аналитики, которая изучает корреляцию между направлениями потоков, событиями, используемыми ресурсами и пользовательскими данными с аномальным поведением, позволяет организациям эффективнее находить их наиболее уязвимые места в сети – ценные информационные активы, которые являются самыми интересными для злоумышленников. Определяя уязвимые области и ресурсы, заранее обеспечивая оценку риска, организации могут своевременно защитить себя от этого нового вида угроз.

Мы живем во взаимосвязанном мире, и безопасность каждой организации оказывает влияние на смежную организацию. В результате этого мы оказываемся в организациях, которые должны иметь правильный набор инструментов безопасности для защиты собственной организации – таким образом помогая своим партнерам обеспечить безопасность. Это приводит к полной более безопасной окружающей среде, которая идет в ногу с развивающимися угрозами. Для более подробной информации о том, как аналитика UEBA может помочь Вашей организации, пожалуйста посетите: www.seceon.com.