ИНФОРМАТИКА

ЗАЩИТА ПРОГРАММНЫХ ПРОДУКТОВ SAP

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Адериха А. В., Скворчевская Я. А.

Пачинин В. И. – канд. техн. наук, доцент

В современных ERP-системах одной из главных задач является защита данных от внешних и внутренних вторжений. Причем эта задача зачастую нетривиальна и ресурсозатратна. Это заставляет внимательнее изучить стандартные средства SAP по защите своего программного обеспечения .

Более 183 тысяч человек пользуются услугами компании SAP по всем миру. Расширяющееся с каждым годом применение систем управления предприятием SAP, систем in-memory, баз данных типа SAP HANA и облачных технологий на их основе, все чаще заставляет возвращаться к вопросу сохранения информационной безопасности.

На конференции BLACK HAT 2012 исследователь сканера безопасности ERPScan Александр Поляков использовал атаку, известную как «подделка ответа сервера» (server-side request forgery (SSRF)), которая успешно прошла внутреннюю систему безопасности SAP и провоцировала переполнение буффера в SAP kernel. Эта же уязвимость была найдена в Java Virtual Machine, что ставит под угрозу системы основанные на XML и J2EE. Такие атаки недоступны для обнаружения системами IDS и большинством брандмауэров. Однако, если уязвимость не является уязвимостью нулевого дня, то в этих случаях пользователь программных продуктов SAP может не только использовать вышеописанные средства, но и рассчитывать на централизованную поддержку сервисами компании SAP AG, которая, например, уже устранила уязвимость SAP вида SSRF.

Эти сервисы позволяют провести детальный анализ информационной безопасности SAP, который в свою очередь позволяет: уменьшить риск системного вторжения; обеспечить конфиденциальность бизнес-данных системы; подтвердить подлинность пользователей; существенно снизить риск дорогостоящих простоев из-за взаимодействия с пользователем.

Проведение оптимизации информационной безопасности SAP в докладе предлагается начать со следующего. Во-первых, существует ряд инструментов и/или услуг, разработанных компанией SAP AG, которые позволяют получить представление о том, насколько безопасно ваше SAP решение в данный момент.

Во-вторых, «Стандарт безопасности операций SAP (SSOS)» представляет обзор основных областей информационной безопасности при выполнении операций SAP и рекомендации по ключевым операциям для всех областей. Этот стандарт был разработан специально для информационной безопасности SAP операций в системе. Он структурирован в виде карты блоков. Каждый блок дает возможность получить информацию по каждой отдельной сфере и может дать ссылки на детальную информацию непосредственно на SAP Service Marketplace, SAP Help Portal, SCN, SAP Notes. Цель этого стандарта – дать пользователю список действий, необходимых для обеспечения безопасности системы, уделить основное внимание действиям (вместо технологий), и тем самым получить быстрые и прагматичные решения ситуаций по защите информации в SAP.

В-третьих, «Sap Security Engagement» всегда доступен и помогает клиентам сопровождать безопасность их среды SAP. Для поддержки корпоративных клиентов существует большое количество сервисов, которые помогают обслуживать безопасность в SAP-системе. К ним относятся: AGS Security Services – конфигурация и оптимизация; AGS Security Service – обновления; EWA – анализ и ключевые системные отчеты; SOS service – оптимизация и валидация конфигурации.

SAP Secure Operation Standard был разработан специально для безопасности SAP операций в систем. Он структурирован в виде карты блоков. Каждый блок дает возможность получить информацию по каждой отдельной сфере и сможет дать ссылки на детальную информацию непосредственно на SAP Service Marketplace, SAP Help Portal, SCN, SAP Notes. Цель этого стандарта – дать пользователю список действий необходимых для обеспечения безопасности системы. SAP уделяет больше внимания действиям (вместо технологий), что позволяет получить быстрые и прагматичные решения ситуаций информационной безопасности.

Не менее важно поддерживать систему в обновленном состоянии. Недавно SAP запустил систему SAP Security Patch Day(SSPD) каждый второй вторник месяца, который специально был синхронизирован с SPD других важных производителей программного обеспечения. В этот день SAP публикует исправления и доработки своего программного обеспечения, которые необходимо применить к системе как можно скорее. Общий порядок должен быть следующим: 1) проверить список обновлений SAP Security Notes на портале SAP Service marketplace; 2) использовать специальный инструмент System recommendations в SAP Solution Manager для проверки обновлений для конкретного решения; 3) при помощи отчета EarlyWatch Alert проверить, какие критические обновления отсутствуют или не установлены в анализируемой системе; 4) воспользоваться ассистентом обновлений (транзакция SNOTE) или оптимизатором поддержки (Maintanance Optimizer), который теперь также показывает необходимые пакеты обновления безопасности для ABAP и JAVA.

Полное и своевременное использование вышеописанных средств позволит достигнуть стабильно высокого уровня безопасности системы.