ПРОТИВОДЕЙСТВИЕ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕВАРИТЕЛЬНОМ ЭТАПЕ ПРОВЕДЕНИЯ АТАКИ

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

Мажейко А.М.

Белоусова Е.С. – канд. техн. наук

В работе представлена актуальность этапа предпосылки проведения атаки на информационную систему и роль пользователя, как наиболее уязвимого компонента системы защиты. Установлено, что для решения данной проблемы необходимо использовать дополнительные автоматизированные или административные блоки принятия решений.

Как известно, хакерская атака представляет собой набор определенных последовательных действий для достижения определенной цели. Порядок базовых этапов приведен на рисунке 1.

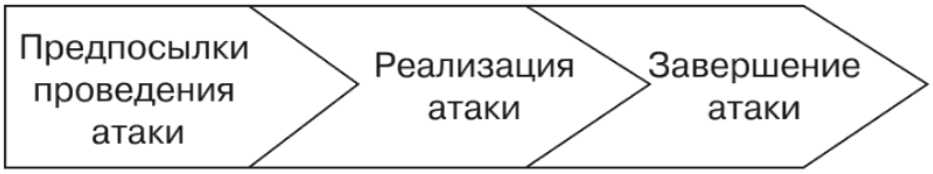

Рисунок 1 – Этапы проведения хакерской атаки [1]

Начиная от исследования и зондирования атакуемой системы, получения к ней доступа и набора необходимых прав и до реализации непосредственной атаки с последующим «заметанием» следов. Существующие системы защиты информации позволяют ставить ограничительные барьеры для действий на каждом из этапов. Однако подавляющее большинство используемых средств защиты направлено на предотвращение атак на этапе «Предпосылки проведения атаки».

Существование термина «человеческий фактор» ставит под угрозу большинство систем защиты. Приведем несколько примеров:

– непреднамеренная загрузка вредоносного программного обеспечения легитимным пользователем на компьютер и последующее неправомерное пользование ресурсами корпоративной сети злоумышленником;

– компрометация ключа доступа к системе (логина, пароля и др.);

– умышленное предоставление доступа нелегитимному лицу легитимным пользователем и последующая эксплуатация уязвимости («исправить ошибку на компьютере», «установить приложение» и прочее).

В приведенных примерах есть общая уязвимая точка – пользователь. Тем или иным способом он является добровольным проводником хакера для получения доступа к системе. Уязвимость состоит в том, что первичные этапы защиты – межсетевые экраны, парольная защита, системы обнаружения вторжений (IDS) – в данном случае оказываются бессильными и пропускают угрозу, т.к. по сути воздействие распознается как действие зарегистрированного пользователя. Пострадавшая организация в данном случае может обнаружить проблему далеко не сразу, даже при наличии в ее штате работников по защите информации и последующем анализе деятельности пользователей. Таким образом для решения проблемы требуются дополнительные технические средства, направленные на выявление необычной деятельности пользователей, и добавление дополнительного блока принятия решений (автоматизированным или административным). В случае автоматизированного решения допускается «жесткий» и «мягкий» подход. Под «жестким» понимается блокировка доступа пользователя к ресурсу до момента снятия блока администратором. В «мягком» подходе используется запрос дополнительных аутентификационных данных пользователя, которые не используются в базовом режиме работы.

Учитывая вышеперечисленную проблему можно утверждать, что разработка и совершенствование средств анализа поведения пользователей в информационной среде является перспективным продолжением развития технологий защиты информации. Здесь можно наблюдать несколько преимуществ. В первую очередь данное направление позволяет автоматизировать процесс реагирования на нетипичное поведение пользователей, а также внутренних нарушителей. Во-вторых, информирование администратора сети или администратора защиты информации становится своевременным и приводит к более быстрому и точному устранению угрозы.

Список использованных источников:
1. Шаньгин, В.Ф. Защита компьютерной информации / В.Ф. Шаньгин. – М. : ДМК Пресс, 2010. – 544 с.