Индустрия ИТ—безопасности изобилует множеством технологий, которые работают, но делают недостаточно, - технологий, которые продаются, даже если они не особенно эффективны с точки зрения затрат. Одной из наиболее распространенных технологий безопасности, которая обычно не является экономически эффективной, является система обнаружения и предотвращения вторжений. Некоторые поставщики могут убедить вас в том, что такая технология нужна каждой компании, но я в этом не уверен. В частности, я считаю, что небольшим компаниям следует тщательно продумать, действительно ли это будет экономически эффективным решением.

Идея сетевых систем обнаружения и предотвращения вторжений (NIDS и NIPS, соответственно) звучит довольно привлекательно. Установите в своей сети флажок, который будет отслеживать весь трафик. Окно выполнит некоторый анализ и сообщит вам, когда вы подвергаетесь атаке (в случае NIDS), или даже автоматически отбросит трафик злоумышленника (в случае NIPS). Конечно, неплохо иметь представление о том, что происходит в вашей сети, потому что такого понимания у вас раньше не было. Но если вы впервые включите свою обычную систему обнаружения вторжений, вы получите спам. Системы обнаружения вторжений регулярно выдают более 10 000 предупреждений в день. Очевидно, что не все из этих предупреждений соответствуют реальным вторжениям, но очевидно, что для того, чтобы система обнаружения вторжений приносила пользу, вы должны уметь отделять некоторые полезные предупреждения от множества несущественных.

Почему устройства обнаружения вторжений так подвержены спаму? Люди любят говорить о ложных срабатываниях, и, конечно, их много. Однако это далеко не вся проблема, как думают некоторые. Как правило, плохие парни постоянно рыщут по Интернету, пытаясь найти проблемы, которые они могут использовать. Да, весь Интернет постоянно подвергается атакам. Например, любой, кто использует сервер с включенной аутентификацией по паролю, заметит множество попыток входа в систему. Злоумышленникам действительно удается взламывать компьютеры, подбирая пароли, поэтому сообщение об этом устройством обнаружения вторжений, безусловно, не является ложным срабатыванием, но большинство таких попыток атаки заканчиваются неудачей. Однако некоторые из них могут быть легко успешными, если у вас есть пользователи с очень плохими (или пустыми) паролями.

Поэтому не обязательно игнорировать все. То, что технологии NIDS и NIPS создают много помех, которые не связаны с ложными срабатываниями, не означает, что ложные срабатывания не являются проблемой. Это, безусловно, так — согласно распространенным сообщениям, многие устройства могут выдавать тысячи ложных срабатываний в день. Но дело в том, что даже если вы сможете избавиться от всех ложных срабатываний, вы не избавитесь от высоких затрат на управление. Для снижения количества предупреждений требуется много работы. Вы должны разобраться в каждом классе проблем, что требует времени.

Весь процесс “настройки” - это очень дорогостоящие первоначальные затраты. И даже после настройки могут возникнуть значительные текущие затраты на просмотр данных о предупреждениях, которые вы, возможно, захотите просмотреть. Например, некоторые пользователи могут захотеть попытаться соотнести неудачные входы в систему по SSH с другим сетевым трафиком, который может указывать на успешное вторжение (будь то вручную или с помощью продукта для управления событиями безопасности). Сами по себе первоначальные затраты достаточно велики, поэтому большинству малых и средних предприятий нет смысла заниматься подобными вещами.

Допустим, вы управляете сетью из 40 пользователей по корпоративной DSL-линии. И давайте предположим, что вы получаете свои NIDS / NIPS и каким-то образом умудряетесь покрыть первоначальные расходы, и настраиваете систему таким образом, чтобы количество

сообщений, которые вы видите и по которым вам нужно принять меры, сократилось до 30 в день. Допустим, на изучение каждого сообщения уходит всего 5 минут. Если ваша команда тратит на решение проблемы 2,5 часа в день, это потенциально обойдется в 30 тысяч альтернативных издержек в год (время, в течение которого ваш ИТ-персонал мог бы работать более продуктивно).

Действительно ли ваша команда тратит в среднем 2,5 часа в неделю на борьбу с инфекциями? И даже если это произойдет, сможет ли система NIDS/NIPS на самом деле избавить вас от затрат на очистку или просто ускорить их устранение?? Короче говоря, экономическая ситуация для малого и даже среднего бизнеса выглядит не очень хорошо. Но на предприятии они, как правило, имеют смысл. Существует большая терпимость к первоначальным затратам и даже к текущим затратам, поскольку наличие даже полудюжины человек, тратящих свои дни на сбор данных системы предотвращения вторжений, может иметь больше смысла для мониторинга сети из 40 000 пользователей, чем тратить деньги на одного человека для мониторинга 40 пользователей.

Единственный способ, при котором есть хоть какая-то надежда на то, что NIDS / NIPS будут экономически эффективными для малого бизнеса, - это если они смогут каким-то образом извлечь выгоду из масштаба. В этом заключается вся идея управляемых служб безопасности (MSS), предлагаемых такими компаниями, как Symantec (благодаря приобретению Riptech), BT Counterpane и VeriSign (благодаря приобретению Guardant). Если эти ребята будут отслеживать и анализировать данные более чем 40 000 пользователей, как если бы они были одной большой компанией, они смогут выполнить эту работу довольно дешево. Если бы у них было 400 компаний по 100 пользователей в каждой, общая стоимость была бы намного больше, потому что у этих компаний не было бы эффекта масштаба.

Вместо этого одна крупная компания могла бы предложить услугу компаниям, состоящим из 100 человек, по более низкой цене, чем они могли бы сделать это сами. Им не пришлось бы тратить время на обучение людей, оплачивать расходы на оборудование или сталкиваться с поломками машин. Но даже управляемый сервис стоит столько денег, что, вероятно, подходит не всем компаниям. Если у вас есть собственные сетевые серверы, доступные через Интернет, это может стоить затрат. Но если вы предоставляете кому-то другому разместить ваш веб-сайт, а у вас нет других ресурсов, кроме настольных компьютеров, которыми пользуются ваши сотрудники, возможно, не стоит даже передавать обнаружение вторжений на аутсорсинг поставщику управляемых услуг. Вместо этого вы можете поместить своих пользователей за сетевой маршрутизатор, и тогда внешний мир не сможет получить доступ к вашим компьютерам, если только кто-то в сети не сделает что-то, чтобы заразить вашу сеть.

Никто извне не сможет проникнуть в сеть, если его туда не пригласят. Кроме того, традиционные AV-системы должны как минимум так же эффективно выявлять угрозы на ранней стадии, как и устройства обнаружения вторжений. Конечно, вы все еще можете осуществлять мониторинг вторжений, но поскольку злоумышленник ничего не сможет увидеть (пока ваши пользователи не подключатся к злоумышленникам или не откроют какое-либо вложение от одного из них), как правило, более экономично потратить свой бюджет на обеспечение безопасности на другие цели. Руководя малым бизнесом, я бы с большой осторожностью относился к расходам на продукты или услуги для мониторинга вторжений, прежде чем увидел бы реальную экономическую выгоду — мне нужно было бы потратить достаточно средств на борьбу с вторжениями, которые явно можно было бы предотвратить, чтобы оправдать расходы.

Если у вас действительно есть потребность в услугах, которые обычно предоставляются с помощью выделенных ИТ-серверов (таких как почтовые серверы и веб-сайты), вы всегда

можете контролировать эти расходы, поручив их кому-то другому. Зачем платить за запуск и администрирование собственных веб-серверов (кстати, гораздо дешевле защитить кластер компьютеров, предназначенных для предоставления только одной услуги), когда вы можете просто разместить свой контент и предоставить кому-то другому решать проблему безопасности? Если ответ заключается в том, что у вас много серверных приложений, то почему бы вместо размещения контента в облаке не разместить свои приложения в облаке?

Пусть Amazon или Google позаботятся о безопасности. Конечно, вы должны доверять им, чтобы они хорошо справились с этой работой, но крупные игроки, как правило, могут продемонстрировать свои методы и успехи в защите инфраструктуры, которой они управляют. Для малого и среднего бизнеса это, как правило, отличное решение, поскольку облачные вычисления обладают всеми преимуществами масштабируемости, которые делают их дешевыми для небольших компаний. Наступает момент, когда у вас достаточно масштабируемости, чтобы это стоило делать самостоятельно, но это не относится ко многим людям.

Подводя итог, можно сказать, что NIDS / NIPS хорош для крупных игроков, но, как правило, слишком шумный, чтобы быть экономически выгодным для всех остальных. Управляемые сервисы могут помочь магазинам среднего размера снизить затраты, но для эффективного использования NIPS, даже если они управляются, требуется не только инфраструктура, но и постоянные инвестиции денег и времени - две вещи, которых обычно не хватает мелким предприятиям. И у них есть лучшие альтернативы, такие как облачные технологии, или они просто обходятся без них, неся расходы по мере необходимости.