Мониторинг сети как важнейшая составляющая ИТ-безопасности

Информационный документ

Автор: Даниэль Зобель, руководитель Отдела разработки программного обеспечения компании Paessler AG

Опубликовано: июль 2013 г.

Содержание

Введение

По результатам опроса, проведенного компанией Paessler AG, компании хотят повысить свою защищенность от текущих и будущих кибер-угроз и других видов ущерба. Приблизительно 1200 пользователям был задан вопрос об использовании ПО Paessler в PRTG Network Monitor. Результаты опроса показали, что 75% из числа опрошенных пользователей считают этот инструментарий важным компонентом безопасности своих сетей. Этот документ подчеркивает роль мониторинга сети как дополнительного компонента безопасности в сетях компаний, где могут возникнуть требующие решения проблемы.

Текущее положение дел

ИТ-безопасность: ситуация в мире

Исследования по безопасности ИТ показывают, что компании ведут определенную профилактическую работу, касающуюся безопасности. Однако киберпреступники постоянно разрабатывают более изощренные цифровые угрозы, которые могут реализовываться различными способами.

В 2013 г. было проведено исследование по 41 параметру, которое показало, что жертвами киберпреступлений стали две трети интернет-пользователей, т.е. более 1,5 млн. новых жертв ежедневно.

Серьезную угрозу для корпоративной информационной безопасности представляет использование мобильных устройств. По данным Trusted Mobility Index, опросившего 4000 человек из США, Великобритании, Германии, Китая и Японии, 41% респондентов, использующих персональные устройства по работе, делают это без разрешения своего работодателя, а одна треть ИТ-специалистов отметила, что их компании уже испытали на себе угрозы безопасности, связанные с мобильными устройствами.

По данным, приводимым Ponemon Institute, нарушения правил безопасности обходятся компаниям в среднем в 7,2 млн. долл. США на инцидент, число которых в последние годы неуклонно растет. Около 85% всех американских компаний пережили одну или несколько утечек данных, и из них более трети до сих пор не имеют формализованного процесса по предотвращению новых нарушений безопасности.

По некоторым оценкам, глобальный ущерб от киберпреступлений может превышать 1 трлн. долл. США. Вот почему сегодня компании должны значительно повысить приоритет мер по обеспечению безопасности своих ИТ-инфраструктур.

Защита ИТ-систем

Многие компании полагают, что для защиты ИТ-инфраструктуры достаточно надежного брандмауэра и современного антивирусного сканера. Тем не менее, киберпреступники разрабатывают все более изощренные методы доступа к компьютерам и серверам компаний. Порой ПО безопасности распознает внедрившихся троянов, червей и т.п. только тогда, когда уже слишком поздно. Если угроза получает доступ к одному-единственному компьютеру в сети компании, то это, как правило, только вопрос времени – когда будет скомпрометирована вся остальная

система.

Целью, как правило, является манипулирование данными либо их уничтожение, или захват вычислительных мощностей для последующего использования в преступных целях. Если из-за атаки с помощью вредоносного ПО произойдет отказ внутренней системы компании, то не будет работать ни деловая связь между офисами компании, ни обработка заказов, ни связь с клиентами. Администраторы при этом сталкиваются с трудоемкой проблемой поиска точного источника заражения. Какие компоненты системы безопасности отказали? Какие подсистемы или компоненты были атакованы вредоносным ПО? Могут ли быть другие причины у отказов одиночных систем?

Чтобы избежать подобных инцидентов, ИТ-инфраструктура нуждается в полной защите.

Для этого у компании должен быть комплексный подход к ее ИТ-безопасности. Помимо брандмауэров и антивирусных программ, частью систем безопасности должны стать и другие меры, такие как ПО для шифрования, ПО для обеспечения безопасности данных, контент-фильтры, сканеры портов и другой инструментарий.

Кроме того, для гарантий полной защиты сети, не следует пренебрегать мониторингом сети в качестве дополнительной меры безопасности. Направленное использование решений такого типа может значительно повысить уровень безопасности ИТ-среды.

Сетевая система раннего оповещения

Система мониторинга сети, как правило, служит для контроля целиком всей ИТ-инфраструктуры, со всеми устройствами и системами. Администраторы могут контролировать все, что использует определенный интерфейс и обменивается информацией о своем состоянии по стандартному протоколу. ПО для мониторинга должно просто установить контакт с устройствами или службами, использующими IP-адреса, после чего оно сможет получать информацию о текущем состоянии конкретных устройств.

Это позволит ИТ-отделу в любое время быть в курсе состояния всех сегментов ИТ-инфраструктуры. Цель заключается в обеспечении максимальной доступности и оптимальной производительности в сети. Для этого система мониторинга сети должна охватывать три аспекта, относящихся к безопасности:

- мониторинг имеющихся систем безопасности;
- выявление необычных вхождений в сеть;
- контроль параметров окружающей среды.

Компании, имеющие насколько различных «площадок», могут использовать для контроля их состояния «удаленные зонды» всех трех категорий. Такой «зонд» представляет собой небольшую программу, предназначенную для контроля удаленной сети изнутри и пересылки данных мониторинга на центральный сервер системы. Благодаря этому, хорошее ПО сетевого мониторинга позволяет отслеживать любое количество сетевых компонентов, находящихся как в основной сети, так и в отдельных филиалах компании. Компоненты, называемые «датчиками», настроены на мониторинг различных параметров сетевых устройств и соединений. Таким образом, администратор видит со своего места работы всю сеть целиком.

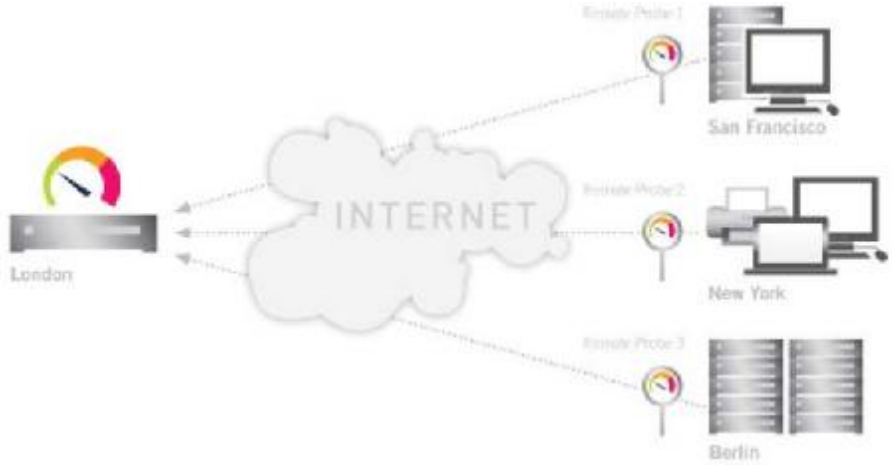

Иллюстрация. Мониторинг нескольких «площадок» с помощью «удаленных зондов»

Если ПО для мониторинга замечает отказ или необычное явление, оно автоматически отправляет уведомление ответственному системному администратору – в виде текстового сообщения и (или) по электронной почте. Таким образом, администраторы, независимо от их местонахождения, всегда сразу же получают информацию об инцидентах и могут оперативно отреагировать на ситуацию

В системе раннего предупреждения ПО для мониторинга используются соответствующие заданные пороговые значения. При их превышении система подает соответствующий сигнал. Администратор может держать активным постоянное подключение к ПО для мониторинга через веб-интерфейс или приложение для смартфона, и сразу же проверить все сигналы при получении уведомления. Затем он может проанализировать тяжесть проблемы и принять соответствующие меры на основании текущих данных мониторинга.

Мониторинг вопросов безопасности

ИТ-администраторы должны иметь возможность так же быстро реагировать на возможные атаки с использованием вредоносного ПО. Если установленные антивирусные решения и брандмауэры вовремя не обнаружат такую атаку, то нанесенный ущерб нанесенный может принести к простою всех бизнес-процессов. Поэтому администраторы могут только реагировать на проблемы, вместо того, чтобы предпринимать активные меры для предотвращения проблем еще до их возникновения. Дело в том, что брандмауэров и антивирусных сканеров не всегда достаточно, чтобы гарантировать всестороннюю защиту сети. Компании, интегрирующие решения для сетевого мониторинга в свои стратегии безопасности, способны обнаруживать потенциальную угрозу своим сетям еще на ранних стадиях.

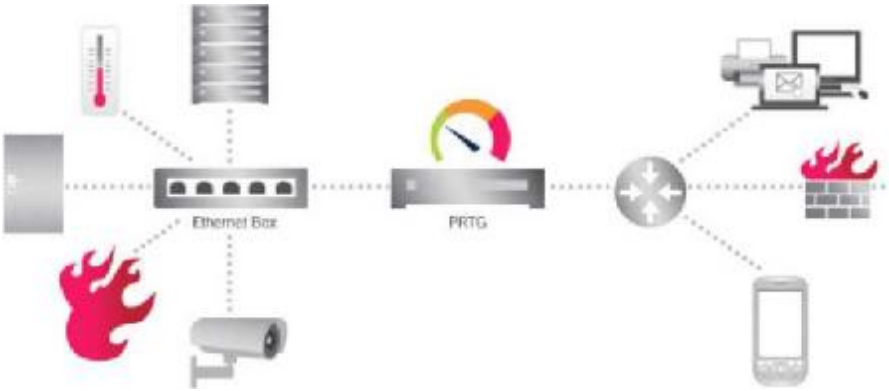

Иллюстрация. Гарантия полной безопасности сети.

Регулярно проверяйте используемые брандмауэры и антивирусные сканеры

Важной задачей, решаемой с помощью сетевого мониторинга, является контроль надежности имеющихся систем безопасности, таких как брандмауэры и антивирусное ПО. Например, ПО для мониторинга может круглосуточно собирать подробную информацию о производительности и состоянии брандмауэра. При неработающем должным образом брандмауэре возрастает риск атаки на сеть с использованием вредоносного ПО.

Иллюстрация. ПО для мониторинга контролирует состояние брандмауэра.

Такие атаки вредоносного ПО могут иметь следующие последствия: начинают случайным образом запускаться программа или открываются те порты, которые должны быть закрыты. Во избежание этого, администраторы получают уведомления об аномальном поведении брандмауэра еще на ранних стадиях. ПО для мониторинга может также проверять, например, антивирусные программы, работающие на центральном сервере электронной почты. Дает компании быть уверенность, что используемые антивирусные сканеры постоянно активны и работают. Решение для мониторинга использует специальные датчики для контроля работы Центра безопасности Windows, позволяющие убедиться, например, что антивирусные сканеры

и программы на каждом компьютере внутри компании обновлены и работают без проблем. Это гарантирует, что клиентские компьютеры также будут постоянно защищены от вредоносного ПО.

Заторы в сети как индикатор проблем

Решения для мониторинга сети помогают администраторам отслеживать полосу пропускания выделенных линий, сетевых соединений, устройств (маршрутизаторов, коммутаторов) и т.п. Детальный мониторинг использования полосы пропускания также может служить косвенным инструментом обнаружения атак вредоносного ПО. Признаком такого нападения может быть замедление отклика от приложений и веб-сайтов, вызванное вредоносным ПО, занимающим значительную часть полосы пропускания. Чтобы обнаружить эти несоответствия, ПО для мониторинга контролирует различные IP-адреса, порты (номера портов), протоколы и т.п. с помощью перехвата пакетов или датчиков потока данных. Датчики потока накапливают отправленные данные и пересылают их для анализа и оценки в ПО для мониторинга. Администратор может проанализировать данные и распознать проблему на ранней стадии, что позволит сразу же предпринять шаги по ее устранению.

Такой тип мониторинга полосы пропускания особенно подходит для сетей с большим трафиком. Необычные явления или активность, например, при атаке вредоносного ПО, могут быть распознаны, если использование полосы пропускания превышает заданные пороги или сильно отличается от средних значений и обычных колебаний. В этом случае администратор может использовать ПО мониторинга для проверки, какой IP-адрес, подключение или протокол использует более широкую полосу пропускания, и соответственно отреагировать.

Мониторинг параметров физической среды

Мониторинг не в последнюю очередь способствует укреплению безопасности благодаря тому, что позволяет отслеживать обстановку в помещениях и окрестностях. Специальные устройства с датчиками дыма или газа сообщат о возгораниях и тому подобных происшествиях еще на ранней стадии развития инцидента. Кроме того, датчики в здании могут быть настроены на включение сигнала тревоги при разблокировке запоров дверей, окон или серверных стоек. ИТ-администраторы могут даже измерять напряжение с помощью соответствующего оборудования и передавать эти данные в ПО сетевого мониторинга, которое в свою очередь отслеживает колебания в питающей сети и уведомляет об этом администраторов. Благодаря большому количеству параметров мониторинга, ИТ-специалисты всегда знают, работает ли их сеть в безопасной среде, и не требуются ли кратко-, средне- или долгосрочные изменения.

Анализ результатов

Высококачественные решения для мониторинга сети сводят все данные мониторинга в отчеты, а так же визуализируют их в виде графиков или информационных панелей. ПО объединяет указанные значения для каждого компонента и системы в удобные для чтения отчеты. В отчете для администратора фигурирует не только работа

брандмауэра и антивирусного сканера, но и сервисные параметры, включая текущую загрузку процессора и оперативной памяти для всех серверов и компьютеров.

Кроме того, ИТ-отделу видна доступность всех сетевых устройств. В отчет также включаются важные тенденции, касающиеся использования сети и полосы пропускания. При необходимости, администратор может сравнивать текущие и архивные данные для различных ситуаций. Если текущие данные выглядят хуже, чем архивные, то это указывает на необходимость оптимизации. Используя автоматический анализ данных мониторинга, администраторы могут обнаруживать похожесть поведения и взаимосвязи между различными датчиками и, таким образом, выявлять ранее неизвестные взаимосвязи между отдельными компонентами сети. Анализ архивных данных, а также выявление датчиков с похожими моделями поведения особенно полезно при проведении сравнительных исследований сложных сетей, с целью изучения точных уровней и видов нагрузки на сеть, а также для ликвидации возможных брешей в защите.

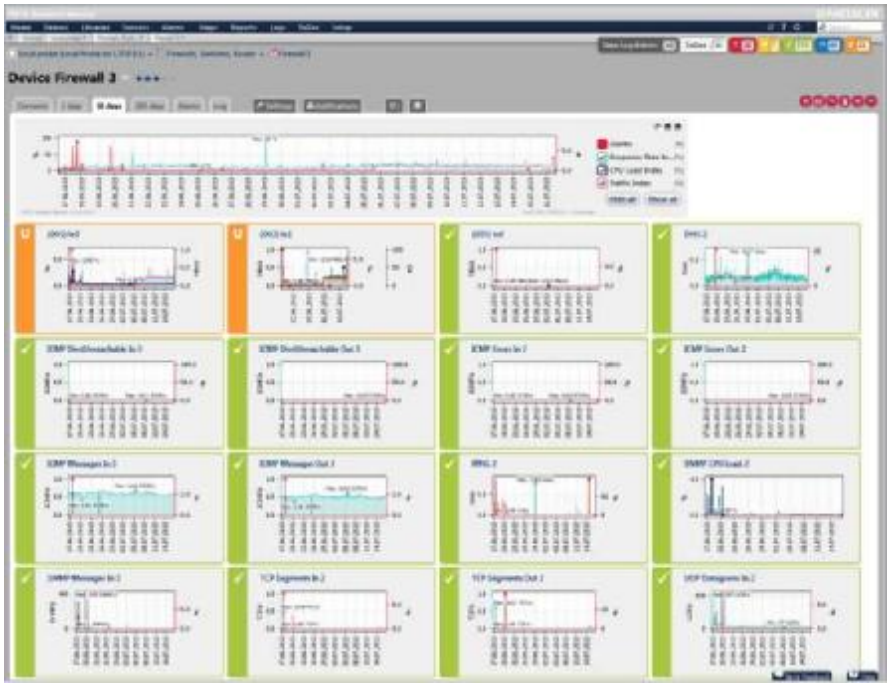

Иллюстрация. Графики облегчают анализ данных мониторинга.

Заключение

Только стратегия безопасности, учитывающая все аспекты, может обеспечить компаниям достаточную защищенность в том, что касается управления рисками. Мониторинг сети является дополнительным, стратегически важным модулем системы ИТ-безопасности, который должен стоять выше и вне использования брандмауэров и антивирусных сканеров. Для обеспечения максимально возможной защиты всей сети компании от атак вредоносного ПО или сбоев, должны контролироваться все ИТ-объекты и площадки. Выявление тенденций и необычного поведения является важным фактором в деле распознания угроз. ПО для мониторинга сети позволяет выстроить систему раннего предупреждения, что делает его полезным дополнением к стратегии безопасности и помогает компании добиться желаемого уровня

безопасности и контроля.

О компании Paessler AG

Компания Paessler AG является отраслевым лидером в области поставок наиболее мощных, доступных по цене и простых в использовании решений для сетевого мониторинга и тестирования. Предлагаемый компанией пакет достаточно простых программных продуктов обеспечивает комфорт, уверенность и удобство в работе для предприятий любых размеров – от Small Office/Home Office (SOHO) до крупных предприятий, в число которых входит более 70% компаний из списка Fortune 100. Компания Paessler находится в Нюрнберге, Германия, и располагает клиентской базой, насчитывающей более 150 000 работающих инсталляций своей продукции. Основанная в 1997, Paessler AG по-прежнему остается частной компанией и является признанным членом Cisco Developer Network и VMware Technology Alliance Partner.

Бесплатные и бесплатные ознакомительные версии всех продуктов компании можно загрузить с сайта www.paessler.com.

Paessler AG

Bucher Str. 79a, 90419 Nuremberg, Germany, www.paessler.com, info@paessler.com

VAT-ID: DE 217564187

TAX-ID: FA Nuremberg 241/120/60894

Регистрация: Суд первой инстанции, Нюрнберг, HRB 23757

Генеральный директор/Главный исполнительный директор: Дирк Паесслер, Кристиан Туардава

Председатель: Д-р Марк Роессель

***Примечание**:*

WP/20130906/SECURITY/EN