Аналитическое чтение

Дедков Сергей

2015

Содержание

1 Human-Centered Study of a Network Operations Center: Experience Report and Lessons Learned

Существует значительный риск в отказе доступа медицинскому работнику, который хочет изучить медицинскую карту пациента. Для снижения рисков работникам даны большие полномочия в этом плане. Работники при этом могут пользоваться своими полномочиями не в медицинских целях. Журналы аудита больницы слишком велики, чтобы проверять вручную, поэтому автоматизация необходима для поддержки отчетности. Ведение журналов аудита, нужно чтобы понять роль и рабочие потоки, развивать надежное обнаружение аномалий и безопасные средства управления доступом.

2 Improving Efficiency of Spam Detection using Economic Model

Одна из угроз обществу пострeдством сети Интернет - спам. Многие методики обнаружения спама - анализ почтового траффика, в виду того, что спам имеет свойство изменять его. Настройка детекторов по обнаружению спама - сложная задача, т.к. обычные письма в некоторых случаях можно принять за спам. Таким образом, погнавшись за увеличением безопасности, существует возможность навредить обычной почте.

Автор статьи описывает введнеие новой метрики для обнаружения спама и предлагает использовать Экономическую Модель, для обнаружения спама, котороя могла бы достаточно тосно отличить спам от обычных писем.

Суть метода заключается в том, что спамеру нет нужды рассылать спам, затрачивая на него средства, которые в последствии не оправдают резултат. спаммеру придется разослать в десятки раз больше писем, чем имеющихся у него адресов.

Авторами был проведен анализ данного метода. Набор данных для анализа состоял из 75000 обычных электронных писем и 3 миллионов спам-писем. Анализ проводился по 4 характеристикам:

- inter-departure time (IDT) - время между двумя последовательными письмами
- emails per recipients (EPR) - писем на получателей
- email size (ES) - размер письма
- distribution of new recipients (DNR) - частота новых получателей

Так же были изучены рынки ботов для отсылки спама и стоимость их услуг.

В итоге с 70% вероятностью детектор на основе IDT определял спам.

В статье описывается новизна данного подхода, определение функции вычисления спама и экономическая модель, тестирование производительности такого детектора и будующие направления развития данного подхода.

3 Enterprise Risk Assessment Based on Compliance Reports and Vulnerability Scoring Systems

В данной статье, авторы представили объективную метрику для оценки риска кибератак на основе отчетов о безопасности от организаций повсеместно в своей работе использующих сети. Такая модель рассматривает различные факторы риска, включая распределение уязвимостей, зависимость между ними, и конфигурацию сети. Авторы пользовались языком Протокола Автоматизации Контента Безопасности (SCAP) и системой измерения по изучению уязвимостей. Также авторы описали План оценки для проверки вводимой метрики.

Security Content Automation Protocol (SCAP) обеспечивает стандартные технические требования, чтобы сообщить информацию о безопасности. Extensible Configuration Checklist Description Format (XCCDF) спецификация SCAP, определяет язык, чтобы описать контрольные списки безопасности и собрать результаты соблюдения предназначенных систем. Модели Risk Estimation Risk определяют факторы риска, которые будут оценены и отношения среди них.

4 Protecting Enterprise Networks through Attack Surface Expansion

Поверхность атаки - ценная метрика, которая помогает администраторам корпоративных сетей оценить риск и безопасность всей сети. Поверхность атаки по сети — общепринятый термин для описания уязвимости сети. Многие сетевые нападения проходят через уязвимые приложения, и можно существенно уменьшить площадь атаки, сократив число активных приложений в сети. Суть подхода авторов для увеличения безопасности состоит в увеличении внешней поверхности атаки, для того, чтобы злоумышленники не могли определить реальную внетреннюю поверхность атаки. Для этого администраторами создается фиктивная сеть со слабыми местами, которая полностью контролируется ими. Такой подход называется attack surface expansion (ASE).

Рассмаотрены варианты с использованием:

- Virtual Identities

- Secret Moving Proxy

- Dynamic Virtual Networks

Нападая на приманку можно потратить массу времени и усилий, а в результате ничего не добиться.

5 Выводы

Риски кибернападения в настоящее врем очень велики. Существует множество аспектов которые требуют детального изучения. Важно уметь оценивать риски таких нападений, и вовремя предотвращать их. Для анализа рисков нападений специалистами вводятся специальные метрики, позволяющие определить степень опасности. Такие оценки и анализ киберпреступлений позволяют в дальнейшем определить методы борьбы с ними и предотвращения. Так, например, вводятся новые средства борьбы с кибератаками. Один из таких подходов - attack surface expansion (ASE), который позволяет запутать атакующих, чтобы они не добились своих преступных целей, путем расширения поверхности атаки. Вводятся новые инструменты анализа спам писем, которые учитывают новые факторы, такие, как экономический. В такой области как компютерна безопасность важно постоянно осуществляь анализ текущих атак, чтобы на основе статистики в дальнейшем принимать правильные решения по их предотвращению.