19. CPU side-channels vs. virtualization rootkits: the good, the bad, or the ugly [ToorCon Seattle 2008].
21. Beyond The CPU: Defeating Hardware Based RAM Acquisition, Joanna RutkowskaCOSEINC Advanced Malware Labs.

С. С. Корт

ПЕРЕОБУЧЕНИЕ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Во многих существующих подходах к построению системы обнаружения вторжений обычно используется статическое обучение классификатора [1]. Однако данный процесс подразумевает стационарность распознаваемого процесса. В общем случае данные, поступающие в систему, не являются стационарными по следующим причинам:

– изменение поведения пользователя с течением времени;

– изменение окружения (появление в сети новых компьютеров и сервисов);

– изменение природы атак на систему;

– зависимость поведения пользователя в определенный момент времени от его поведения до этого момента времени.

Список этих причин можно расширить, но уже он показывает, что говорить о стационарности соответствующих процессов в системе некорректно. Как следствие этого, в идеальном случае обучение должно быть динамическим, а система должна быть адаптивной, периодически переобучаясь. Можно выделить три подхода к переобучению системы:

1) Переобучение системы инициируется пользователем. В том случае, если в системе отсутствует переобучение, она может оценивать поведение пользователя, которое можно охарактеризовать как стационарное.

2) Система обучается постоянно. Каждое новое событие вызывает переобучение. Переобучение при поступлении каждого события приводит к необходимости построения самообновляющегося профиля. К достоинствам данного подхода можно отнести преодоление проблемы адекватного описания модели системы, включающего условие стационарности. К недостаткам подхода можно отнести подверженность атакам на механизм обучения и неэффективность подхода, выражающуюся в слишком частой необходимости перестроения базы знаний.

3) Система переобучается при наступлении какого-то особого события. Данный подход к переобучению является адаптивным и устраняющим недостатки предыдущих двух подходов. Переобучение в данном случае выполняется при наступлении некоторого события, после возникновения которого соответствующий процесс не может оцениваться как стационарный и появляется необходимость перестроения базы знаний системы.

Вне зависимости от типа информации, на основании которой обучается система (по нормальному поведению или по данным об атаках), можно выделить три типа операций: разрешенные политикой безопасности, запрещенные политикой безопасности и неопределенные.

С точки зрения системы обнаружения вторжений, неопределенной является операция, которая может быть оценена как принадлежащая и безопасному поведению и поведению нарушителя. Неопределенная операция может выполняться как нарушителем, так и авторизованным пользователем, как безопасной программой, так и разрушающим программным обеспечением. Необходимо отметить, что четко определенная политика безопасности системы должна уменьшать количество неопределенных операций.

Таким образом, факт выполнения неопределенной операции, являясь большой проблемой систем обнаружения вторжений, может служить событием-триггером, по которому целесообразно проводить переобучение системы обнаружения вторжений. Тогда переобучение системы обнаружения вторжений можно выполнять при следующих условиях:

1) если пользователь выполнил запрещенную политикой безопасности операцию: соответствующую аномальному поведению (система обучалась нормальному поведению) или атаку (система обучалась атакам);

2) если пользователь выполнил неопределенную операцию: неспецифицированную как нормальную операцию политикой безопасности или операцию, разрешенную политикой безопасности, которая может быть выполнена при вторжении.

СПИСОК ЛИТЕРАТУРЫ:

1. *Zegzhda P. D., Kort S. S.* Host-based Intrusion Detection System: model and design features // The Forth International Conference, MMM-ACNS 2007. St. Petersburg, Russia. September 13–15. 2007. Proceedings. Communications in Computer and Information Science (CCIS). Springer. Vladimir Gorodetsky, Igor Kotenko, Victor Skormin (Eds.). Vol. 1. 2007. P. 340–345.

А. Б. Костина

ПРАКТИЧЕСКИЕ АСПЕКТЫ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ни одна самая совершенная мера по снижению рисков ИБ не может полностью предотвратить возникновение в информационной среде событий, потенциально несущих угрозу бизнесу организации. Неготовность организации к обработке подобного рода ситуаций может существенно затруднить восстановление нормального функционирования организации и потенциально усилить нанесенный ущерб.

Справиться с данной проблемой может процесс управления инцидентами ИБ. Именно во время работы разных этапов этого процесса проявляются конкретные уязвимости активов организации, обнаруживаются следы атак и вторжений, проверяется работа защитных механизмов, эффективность работы процессов обеспечения ИБ и управления ею.

Внедрение процесса управления инцидентами ИБ на практике может быть связано с рядом проблем, в частности, в организации необходимо наличие четкого определения события и инцидента ИБ. На данный момент существует большое количество международных документов, регламентирующих терминологию данного процесса. Однако, приводимых в них определений этих терминов недостаточно, так как в зависимости от специфики деятельности организации, от ее масштаба, а также от общего уровня зрелости организации по ИБ значения понятий «событие ИБ» и «инцидент ИБ» могут варьироваться.

Важным аспектом успешного внедрения процесса управления инцидентами ИБ является введение классификации инцидентов ИБ. От правильно выбранной классификации зависит то, насколько эффективен будет процесс в целом.