электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.056.5

Обзор моделей и программ мониторинга безопасного поведения пользователей

***Марков Г.А.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Цирлов В.Л., к.т.н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
v.a.matveev@bmstu.ru

Введение

Известно, что наибольшую угрозу активам компании приносят не внешние угрозы, а внутренние в лице собственных сотрудников [1, 5]. Ни одна компания не застрахована от человеческого фактора как в случае преднамеренных нарушениях, так и непреднамеренных. Наибольшую опасность в данном случае несет раскрытие информации, составляющей коммерческую тайну, и персональных данных [3].

Одним из вариантов снижения такого риска есть мониторинг пользовательской активности за рабочим месте [4, 6].

Обзор программ мониторинга

Существует множество продуктов для мониторинга пользовательской активности [2, 7-10]. Приведем примеры наиболее известных программ и составим сравнительную таблицу.

Nagios - программа мониторинга компьютерных систем и сетей с открытым кодом. Nagios предназначена для наблюдения, контроля состояния вычислительных узлов и служб, оповещает администратора в том случае, если какие-то из служб прекращают (или возобновляют) свою работу.

Возможности программы:

- Мониторинг сетевых служб (SMTP, POP3, HTTP, NNTP, ICMP, SNMP);
- Мониторинг состояния хостов (загрузка процессора, использование диска, системные логи) в большинстве сетевых операционных систем;
- Поддержка удаленного мониторинга через шифрованные туннели SSH или SSL;

- Простая архитектура модулей расширений (плагинов) позволяет, используя любой язык программирования по выбору (Shell, C++, Perl, Python, PHP, C# и другие), легко разрабатывать свои собственные способы проверки служб;
- Параллельная проверка служб;
- Возможность определять иерархии хостов сети с помощью «родительских» хостов, позволяет обнаруживать и различать хосты, которые вышли из строя, и те, которые недоступны;
- Отправка оповещений в случае возникновения проблем со службой или хостом (с помощью почты, пейджера, смс, или любым другим способом, определенным пользователем через модуль системы);
- Возможность определять обработчики событий произошедших со службами или хостами для проактивного разрешения проблем;
- Автоматическая ротация лог-файлов;
- Возможность организации совместной работы нескольких систем мониторинга с целью повышения надёжности и создания распределенной системы мониторинга;
- Включает в себя утилиту nagiostats, которая выводит общую сводку по всем хостам, по которым ведется мониторинг.

Munin – программа мониторинга .Состоит из сервера, который устанавливается на одну систему, где будут собираться все данные, и из демона который устанавливается на остальные системы и способствует сбору данных

OpenView — семейство программных продуктов компании Hewlett-Packard по управлению системами и сетями связи. Предоставляет широкие возможности по мониторингу и управлению локальными вычислительными сетями, серверными платформами рабочими местами пользователей. Более 50 программных продуктов, решающих самые разнообразные задачи — от резервного копирования до мониторинга состояния бизнес процессов в реальном времени.

Collectd — это небольшой демон, который каждые 10 секунд собирает статистку об использовании ресурсов системы. Есть возможность сбора статистики для нескольких хостов и отсылка её на сервер, который занимается отрисовкой графиков.

NetXMS – система мониторинга сети. Распространяется по лицензии GPLv2.

Возможности системы:

- мониторинг состояния сетевых устройств;
- мониторинг ПО работающего на серверах;
- сбор статистики по работе сетевых устройств;

- сбор статистики по производительности серверов;
- автоматическое обнаружение новых узлов сети;
- уведомления о проблемах по эл. почте и смс.

OpenNMS – Open Source система мониторинга. Основная функция OpenNMS (Open Network Monitoring System) – мониторинг различных сервисов и внутренних систем сетевого и серверного оборудования. Для сбора информации используются так называемые «коллекторы», работающие по SNMP, HTTP.

	IPv6	Syslog	SNMP	Управление доступом	Автоматическое обнаружение	Метод хранения данных	Лицензия
AccelOps	?	+	+	+	+	PostgreSQL	коммерческая
AdRem NetCrunch	-	+	+	+	+	SQL	коммерческая
AggreGate Network Manager	+	+	+	+	+	MySQL, MS SQL, PostgreSQL, Oracle, Firebird, HSQLDB	бесплатная с ограничениями/ коммерческая
Argus	+	+	+	+	+	Flat file, MySQL	GPL, коммерческая
Avaya VPFM	+	+	+	+	+	MySQL	коммерческая
Cacti	+	+	+	+	+	RRDtool, MySQL	GPL
Centina Systems NetOmnia	+	+	+	+	+	MySQL	коммерческая
Check MK	?	+	+	+	+	RRDtool	GPL
collectd	+	+	+	+	+	RRDtool	GPL
ExtraHop	+	-	-	+	+	Proprietary	коммерческая
FreeNATS	?	+	-	+	+	MySQL	GPL

Ganglia	?	-	+	-	+	RRDtool	
Glasswire	+	-	+	+	+	Proprietary	бесплатная с ограничениями/ коммерческая
HP Network Node Manager (NNMi)	+	+	+	+	+	PostgreSQL	коммерческая
IBM Tivoli Network Manager	+	+	+	+	+	MySQL, Oracle Database, DB2	коммерческая
Icinga	+	+	+	+	+	PostgreSQL, Oracle Database	GPL
IPHost Network Monitor	+	-	+	-	+	FirebirdSQL	коммерческая
isyVmon	+	+	+	+	+	MySQL, RRDtool	бесплатная с ограничениями/ коммерческая
Kaseya Network Monitor	?	+	+	+	+	FirebirdSQL	коммерческая
Monitorix	+	-	+	+	-	RRDtool	GPL
Munin	+	-	+	?	-	RRDtool	GPL
Nagios	+	+	+	+	+	Flat file, SQL	GPL
NetXMS	-	+	+	+	+	MySQL, PostgreSQL, SQL	GPL
NeuralStar	+	+	+	+	+	MS SQL	коммерческая

CA Nimsoft Monitor	+	+	+	+	+	MySQL	бесплатная с ограничениями/ коммерческая
Observium	+	+	+	+	+	RRDtool, MySQL	QPL, коммерческая
OpenKBM	+	+	+	+	+	Proprietary	коммерческая
OpenNMS	+	+	+	+	+	RRDtool, PostgreSQL	GPL
Opmantek NMIS	+	+	+	+	+	RRDtool	GPL, коммерческая
Opsview	+	+	+	+	+	SQL	коммерческая
op5 Monitor	+	+	+	+	+	Flat file, SQL	бесплатная с ограничениями/ коммерческая
OSI NetExpert	+	+	+	+	+	Oracle	коммерческая
PA Server Monitor	-	+	+	+	+	SQLite, Microsoft SQL Server	коммерческая
PacketTrap	+	+	+	+	+	SQL	коммерческая
Pandora FMS	+	+	+	+	+	MySQL, PostgreSQL, Oracle	GPL, коммерческая
PRTG Network Monitor	+	+	+	+	+	Proprietary	коммерческая
Redcell	+	+	+	+	+	MySQL, Oracle	коммерческая
Scrutinizer	+	+	+	+	-	MySQL	бесплатная с ограничениями/ коммерческая
SevOne	+	+	+	+		MySQL	коммерческая

Shinken	+	+	+	+		MySQL, Flat file, Oracle	GPL
Solarwinds	+	+	+	+		SQL	коммерческая
CA Spectrum	+	+	+	+		MySQL	коммерческая
TclMon	-	+	+	+		RRDtool	BSD
uptime software	?	+	+	+		Oracle	коммерческая
Verax NMS	?	+	+	+		Oracle, SQL,	коммерческая
Zabbix	+	+	+	+		PostgreSQL, Oracle	GPL
Zenoss	+	+	+	+		MySQL	GPL, коммерческая

Характеристики поведения пользователя

Следующие характеристики использовались в программах мониторинга поведения пользователя:

- Время работы/отсутствия/бездействия;
- Количество неверных попыток введения пароля;
- Контроль за документами, отправленными на печать;
- Контроль за просматриваемыми документами пользователя (относится ли документы к его работе);
- Контроль копируемой информации с компьютера (на флешки/отправляемые по сети/снимки экрана);
- Время проводимое на сайтах, не относящихся к работе, а так же анализ таких сайтов (сайты конкурентов, сайты с вирусами, соцсети);
- Анализ устанавливаемых на ПК программ;
- Отключение служб или средств безопасности;
- Изменение параметров программных и аппаратных средств;
- Поисковые запросы;
- Изменение данных учетной записи.

При построении модели поведения пользователя, следует отталкиваться именно от вышеперечисленных характеристиках.

Правила безопасности

На основании характеристик, можно привести пример правил безопасности , которые можно использовать в политике безопасности компании:

- Разграничение доступа по принципу должен знать(пользователь должен иметь доступ только к той информации, которая ему необходима для должностных обязаностей и не более);
- Запретить обычным пользователям устанавливать или вводить изменения в программы;
- Политика парольной системы (введение правил для парольной системы: установление минимальной длинны, обязательное использование спецсимволов и пр.);
- Правила работы с носителями информации;
- Правила работы с почтой;
- Контроль за временем работы (блокировка учетных записей в нерабочее время);
- Запрет вывода на печать критически важных документов;
- Блокировка нежелательных сайтов (соцсети, вредоносные ссылки и пр.);
- Запрет активации и деактивации системных служб.

Выводы

Программы мониторинга пользовательской активности помогут не только сэкономить значительные средства, но и повысить эффективность работы сотрудников. К минусам таких продуктов можно отнести, небольшой функционал. В настоящее время такие программы можно заменить более эффективными средствами в области информационной безопасности, но и стоимость таких средств будет выше. Программы мониторинга пользовательской активности недорогой и практичный вариант снижения рисков, связанных с угрозами исходящих от сотрудников компании.

Список литературы

1. Акулов О.А., Баданин Д.Н., Жук Е.И., Медведев Н.В., Квасов П.М., Троицкий И.И. Основы информационной безопасности: учеб. пособие. М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. 161 с.

2. Бирюков А. Выбираем средство мониторинга удаленных сессий пользователей // Системный администратор. 2013. № 1-2 (122-123). С. 62-65.
3. Гарнаева М.А., Функ К. Kaspersky Security Bulletin 2013 // Вопросы кибербезопасности. 2014. № 3 (4). С. 65-68.
4. Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1 (2). С.28-35.
5. Матвеев В.А., Цирлов В.Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2014 г. // Вопросы кибербезопасности. 2013. № 1(1). С.61-64.
6. Зима В.М., Котухов М.М., Ломако А.Г., Марков А.С., Молдовян А.А. Разработка систем информационно-компьютерной безопасности. СПб.: ВКА им. А.Ф.Можайского, 2003. 327 с.
7. Стефанцов А.Г., Штык А.Н., Раскатова М.В., Тихонова Е.А. Мониторинг действий пользователей в информационных системах отраслевого уровня // Информационные технологии моделирования и управления. 2010. № 3 (62). С. 388-397.
8. Титович С.М., Гринкевич Т.В., Кочурова С.В. Мониторинг использования научных электронных ресурсов в информационном обслуживании пользователей // Научные и технические библиотеки. 2009. № 10. С. 33-37.
9. Трошин С.В. Мониторинг работы корпоративных пользователей // Вопросы современной науки и практики. Университет им. В.И. Вернадского. 2009. № 2 (16). С. 59-71.
10. Цветков А.А. Идентификация профиля пользователя распределенной вычислительной сети на основе активного мониторинга // Электронное периодическое издание Информационная среда образования и науки. 2013. № 17. С. 86-91.