Trend Micro™

Worry-Free™ SecureSite – бета-версия

Защитите свой Интернет-магазин и его клиентов от хакеров, новых угроз и кражи конфиденциальных данных.

Интернет-магазин приносит прибыль и создает деловую репутацию. Однако хакер может атаковать веб-сайт, воспользовавшись известными и новыми уязвимостями, и сделать его владельца невольным соучастником распространения «шпионских» программ или хищения конфиденциальных данных. Это может поставить под угрозу работу магазина, его репутацию, а также безопасность клиентов.

Tested: 02 June, 2008

Worry-Free™ SecureSite — это серверное решение, которое позволяет владельцам Интернет-магазинов сканировать свои веб-сайты на наличие известных и новых уязвимостей. При обнаружении уязвимостей они могут связаться с собственным ИТ-отделом или партнерами компании Trend Micro, чтобы устранить уязвимости в соответствии с рекомендациями TrendLabs℠ — всемирной сети центров, где работают специалисты по безопасности.

Чтобы принять участие в бета-тестировании решения Worry-Free SecureSite, посетите следующий веб-сайт: http://emea.trendmicro.com/emea/products/sb/worry-free-secure-site/sign-up-now/index.php

ОСНОВНЫЕ ФУНКЦИИ

Отслеживание уязвимостей с помощью SecureSite позволит:

- владельцам и клиентам Интернет-магазинов не беспокоиться о безопасности и конфиденциальности данных;
- сохранить деловую репутацию;
- защитить веб-сайты Интернет-магазинов с помощью современных технологий от компании Trend Micro, предназначенных для определения уязвимостей

Защита веб-приложений от компании Trend Micro

- Постоянная проверка веб-сайта на наличие уязвимостей для защиты от атак, связанных со взломами сайтов, SQL-вторжениями, межсайтовым выполнением сценариев или активностью ботов
- Сканирование на наличие уязвимостей в различных веб-приложениях, базах данных и операционных системах в поисках слабых мест, которыми могут воспользоваться хакеры
- Составление отчетов о статусе защиты веб-сайта с помощью веб-консоли. Эти отчеты содержат описание всех уязвимостей и подробные сведения о наиболее опасных из них. Кроме того, возможна настройка параметров уведомлений.

Быстрое развертывание

- Быстрое устранение проблем за счет обращения к постоянно расширяющемуся списку советов об уязвимостях
- **Отсутствие необходимости в установке программного обеспечения или оборудования.** Worry-Free SecureSite — это серверное решение, позволяющее обеспечить безопасность с помощью новейших технологий защиты. Его поддержку и обновление осуществляет компания Trend Micro.

ЗАЩИТА ИНТЕРНЕТ-МАГАЗИНОВ ЗА СЧЕТ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ

Решение Worry-Free SecureSite ежедневно сканирует веб-сайт на наличие уязвимостей следующих типов:

МОШЕННИЧЕСКИЕ И ФИШИНГОВЫЕ ПРОГРАММЫ

- **Межсайтовое выполнение сценариев –** наиболее распространенная технология фишинга, использующая уязвимости веб-сайтов

УТЕЧКИ ДАННЫХ

- **Утечки данных –** раскрытие конфиденциальной информации (комментариев разработчика, пользовательских данных, IP-адресов, исходного кода и т.п.) преступникам
- **Предсказуемые URL-адреса –** поиск конфиденциальной информации на сайтах путем сканирования на наличие забытых страниц
- **SQL-вторжение –** кража баз данных путем внедрения кода в веб-сайты; при помощи этого метода были совершены самые крупные кражи с кредитных карт на сегодняшний день
- **Обратный путь в каталогах –** просмотр не предназначенных для публичного доступа веб-страниц, используя обычную функцию веб-серверов
- **Внедрение операторов XPath –**получение злоумышленниками доступа к XML-документам, содержащим конфиденциальную информацию

НЕСАНКЦИОНИРОВАННОЕ ИСПОЛЬЗОВАНИЕ

- **Неполное ограничение доступа –** приводит к получению неавторизованными пользователями доступа к защищенным областям веб-сайта
- **Злоупотребление функциональностью –** использование функций веб-сайта для раздражения или обмана пользователей
- **Переполнение буфера –**использование уязвимостей веб-сайта для полного перехвата управлением сервера для совершения злоумышленных действий

ПРОГРАММЫ И СЛУЖБЫ

Объекты защиты

- Веб-приложения
- Базы данных
- Сети
- Операционные системы

Отслеживание веб-уязвимостей для защиты от:

- межсайтового выполнения сценариев;
- веб-угроз;
- SQL-вторжений;
- хакерских атак;
- вредоносных программ на языке Javascript;
- фишинга

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

- Защита Интернет-магазинов от хакеров и угроз
- Защита деловой репутации, доверия клиентов и прибылей
- Обнаружение уязвимостей и оказание профессиональной помощи по их устранению
- Помощь владельцам интернет-магазинов в соответствии требованиям отраслевого стандарта по защите данных платежных карт (PCI DSS)
- Помощь в обеспечении бесперебойной работы Интернет-магазинов

ЗАЩИТА ИНТЕРНЕТ-МАГАЗИНОВ ЗА СЧЕТ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ

Служба Worry-Free SecureSite сканирует различные версии перечисленных ниже веб-приложений, баз данных, сетей и операционных систем на наличие угроз безопасности и уязвимостей.

СКАНИРОВАНИЕ	ПРИМЕРЫ	ЗАЩИТА
Веб-приложения и приложения Web 2.0	**Веб-инфраструктура —** Apache, Apache Tomcat, Microsoft™ Internet Explorer, Mozilla FireFox, Microsoft™ IIS, FTP, BEA Weblogic, Adobe ColdFusion, SSH, TELNET и корзины покупателей **Web 2.0 —** приложения JavaScript, AJAX, Adobe Flash **Веб-приложения —** приложения и содержимое, размещаемые на веб-сайте	• Нарушение защиты веб-сайтовза счет использования уязвимостей межсайтового выполнения сценариев • Подмена содержимого • Вредоносные программы на языке Javascript • Уязвимости, которые могут привести к отказу в обслуживании на веб-сайте • Повреждение или кража данных или конфиденциальной информации
Базы данных	Oracle • Microsoft™ SQL Server • Sybase • PostgreSQL • Sun™ MySQL • IBM™ DB2 • IBM™ DB2/400 • Lotus Notes™/Lotus™ Domino™	• SQL-вторжение используется для кражи данных кредитных карт и конфиденциальной информации • Вопросы конфигурации и нарушение политик
Сетевые системы	Брандмауэры Cisco™, IPSec, PPTP, файловая система NFS, DHCP, DNS, LDAP, SNMP	• **Вопросы конфигурации системы (например, использование ненадежных паролей)** • **Несанкционированный доступ к системам**
Операционные системы	Microsoft™ Windows™, Linux, UNIX, Sun™ Solaris™, Mac OS, BSC, IBM™ AIX™, IBM™ AS/400, Novell™ NetWare™	Доступ в операционные системы или нарушение их работы благодаря простым паролям, полномочиям доступа к файлам или доступу к чужим учетным записям

РАСШИРЬТЕ СВОЮ ЗАЩИТУ

Защита ПК, серверов и электронной почты

• Worry-Free Business Security

Серверная защита электронной почты

• InterScan™ Messaging Hosted Security

Службы

• Круглосуточная поддержка семь дней в неделю

СИСТЕМНЫЕ ТРЕБОВАНИЯ

Для правильной работы веб-интерфейса пользователям Worry-Free SecureSite необходимо иметь подключение к Интернету и один из следующих рекомендованных браузеров:

• Microsoft Internet Explorer 6 или более поздняя версия;

• Mozilla Firefox 1.5.x или более поздняя версия

http://emea.trendmicro.com