МОНИТОРИНГ УЯЗВИМОСТЕЙ И УПРАВЛЕНИЕ УСТАНОВКОЙ ИСПРАВЛЕНИЙ (ПАТЧ-МЕНЕДЖМЕНТ)

Своевременная оценка уязвимостей и установка исправлений — для борьбы с целенаправленными и другими типами кибератак

Уязвимости в таких популярных программах, как Java™, Internet Explorer® и Adobe®, — один из основных рисков для информационной безопасности. И это касается не только уязвимостей нулевого дня — в 2014 году 42% инцидентов в корпоративной безопасности были связаны с уязвимостями, которые существовали уже несколько лет[1].

Если вы сами не замечаете уязвимостей, то это не значит, что их не видят киберпреступники. Инструмент патч-менеджмента «Лаборатории Касперского» в среднем исправляет уязвимости за 2-4 дня. Независимые тесты постоянно подтверждают, что наши решения поддерживают самые распространенные приложения и обеспечивают наивысшее в отрасли качество установки исправлений, которая происходит быстрее и вызывает меньше ложных срабатываний по сравнению с решениями других производителей[2].

При этом бизнес с каждым годом все сильнее страдает от кибератак. По оценкам одной из ведущих в мире страховых компаний Lloyd's®, общий ущерб для организаций в результате кибератак составляет 400 миллиардов долларов в год. Исследования «Лаборатории Касперского» показывают, что ущерб в результате кибератак составляет для компаний среднего размера 893 тысячи рублей, а для крупных компаний — 20 миллионов рублей[3]. При этом компании теряют деньги не только напрямую — на то, чтобы устранить последствия инцидента и восстановить привычное функционирование бизнес-процессов, уходят дни и недели. Не стоит также забывать о репутационных потерях.

- **Автоматическое обнаружение уязвимостей**
- **Автоматическое развертывание обновлений и исправлений для ПО Microsoft® и других производителей**
- **Поддержка режима тестирования исправлений**
- **Отложенное развертывание исправлений и установка по расписанию**
- **Оптимизация потребления трафика**
- **Мониторинг результатов установки исправлений**
- **Создание отчетов об уязвимостях и исправлениях**

СВОЕВРЕМЕННАЯ И ЭФФЕКТИВНАЯ ЗАЩИТА

Инструмент мониторинга уязвимостей и установки исправлений «Лаборатории Касперского» действует своевременно, работает стабильно и не влияет на привычные рабочие процессы. Он повышает надежность и эффективность IT-службы, автоматизируя множество задач и снижая время простоев, которые связаны с установкой обновлений ПО. По сравнению с аналогичными инструментами, решение «Лаборатории Касперского» распространяет исправления быстрее, охватывает больше приложений и вызывает меньше ложных срабатываний.

АВТОМАТИЗИРОВАННЫЙ ЦИКЛ МОНИТОРИНГА УЯЗВИМОСТЕЙ

Решение «Лаборатории Касперского» сканирует всю вашу корпоративную сеть, чтобы обнаружить уязвимости, возникшие из-за неисправленных версий программ или операционных систем. Оно автоматизирует цикл мониторинга уязвимостей и установки исправлений, в который входят: Обнаружение уязвимостей • Приоритизация уязвимостей • Загрузка исправлений или обновлений • Тестирование обновлений • Развертывание обновлений • Мониторинг результата • Создание отчетов.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ И КОНТРОЛЬ

Все средства управления защитой рабочих мест, включая оценку уязвимостей и установку исправлений, управляются из единой консоли Kaspersky Security Center.

---

1 Explore The HP Cyber Risk Report 2015
2 Patch Management Solutions Test
3 Данные исследования «Информационная безопасность бизнеса», проведенного «Лабораторией Касперского» и B2B International в 2015 году.

Возможности

ПРОВЕРКА И ОБНАРУЖЕНИЕ
Автоматическая проверка ПО позволяет быстро обнаруживать уязвимости, расставлять их в порядке важности, а затем исправлять. Проверка может производиться в кратчайшие сроки — автоматически или по расписанию в соответствии с требованиями администраторов. С помощью единой политики устанавливаются правила сканирования уязвимостей в программах как Microsoft, так и других разработчиков. Гибкое управление политиками упрощает установку обновленного, совместимого ПО, а также создание исключений, основанных на роли компьютера в корпоративной сети.

ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ
Эффективная оценка уязвимостей позволяет приоритизировать их по степени критичности. Уровень опасности определяется на основе экспертизы специалистов «Лаборатории Касперского» и дополнительных инструментов анализа угроз. В то же время, если обнаруживается, что вредоносная программа использует какую-либо уязвимость, такой уязвимости немедленно присваивается высший приоритет.

ЗАГРУЗКА ИСПРАВЛЕНИЙ И ОБНОВЛЕНИЙ
Решение может автоматически загружать необходимые исправления и обновления с помощью серверов «Лаборатории Касперского». Для обновлений ПО Microsoft решение может также выполнять роль на сервере обновлений Windows® (WSUS). В этом случае оно будет регулярно синхронизировать данные о доступных обновлениях и исправлениях с серверами WSUS и автоматически распространять их по рабочим станциям в корпоративной сети.

ТЕСТИРОВАНИЕ ИСПРАВЛЕНИЙ И ОБНОВЛЕНИЙ
Перед установкой исправлений и обновлений для приложений и операционных систем в масштабах всей организации администратор может их протестировать в локальной среде, чтобы убедиться, что они работают надлежащим образом и не оказывают негативного влияния на производительность системы и продуктивность сотрудников.

Функционал мониторинга уязвимостей и установки исправлений доступен в составе следующих продуктов линейки Kaspersky Security для бизнеса:
- Kaspersky Endpoint Security для бизнеса РАСШИРЕННЫЙ
- Kaspersky Total Security для бизнеса
- Kaspersky Systems Management

По вопросам покупки проконсультируйтесь со специалистами компании Литек - официальным партнером «Лаборатории Касперского».

УСТАНОВКА ИСПРАВЛЕНИЙ
Исправления и обновления могут также быть развернуты автоматически, при этом установку исправлений можно произвести в нерабочее время, благодаря поддержке Wake-on-LAN. Технология Multicast позволяет локально развертывать обновления и исправления в удаленных офисах. В этом случае определенная машина в удаленном офисе получает все необходимые обновления и исправления и распространяет их по другим локальным машинам, существенно экономя потребление трафика.

МОНИТОРИНГ РЕЗУЛЬТАТОВ УСТАНОВКИ
Администратор может производить мониторинг результатов установки исправлений, чтобы убедиться, что уязвимость устранена и исправления функционируют корректно. Если происходит ошибка, администратор получает уведомление о ней. Если обновления были установлены на 100 машинах, администратору не придется искать неполадки на каждой из них — он получает автоматически сгенерированный итоговый отчет.

ОТЧЕТЫ
Решение «Лаборатории Касперского» позволяет администраторам получать отчеты о сканировании, чтобы узнавать о наиболее слабых звеньях сети, отслеживать изменения и быть в курсе происходящего как во всей системе IT-безопасности, так и относительно любого рабочего места в корпоративной сети.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ ИЗ ЕДИНОЙ КОНСОЛИ
Функционал патч-менеджмента «Лаборатории Касперского» — часть единой интегрированной консоли администрирования Kaspersky Security Center, которая поддерживает централизованное управление физическими, мобильными и виртуальными конечными устройствами во всей корпоративной сети с помощью единого интерфейса.
Общая платформа обеспечивает полную прозрачность всех ресурсов сети — не только стационарных компьютеров и ноутбуков, но также смартфонов, планшетов, серверов и виртуальных рабочих станций. Чтобы максимально защитить рабочие места, решение «Лаборатории Касперского» минимизирует время, необходимое для устранения уязвимостей в ОС и приложениях для рабочих станций и серверов на базе Windows, и добавляет дополнительный уровень безопасности для вашего бизнеса.

ЛИТЕК
Тел. (343) 219-73-53, 350-78-76
E-mail: adm@litek.ru
Skype Litek-online
Skype Litek-Sales

KASPERSKY lab