



Один из крупнейших производителей оконных и дверных систем VEKA Rus внедрил решение Cisco Advanced Malware Protection (AMP) for Endpoints

Завершился проект по установке локальных средств защиты информации от вредоносного ПО, разработанных компанией Cisco, для оконечных устройств компании VEKA Rus. С помощью решения Cisco Advanced Malware Protection (AMP) for Endpoints удалось повысить уровень безопасности оборудования сотрудников предприятия, находящихся в Москве, Новосибирске, Хабаровске, Алматы (Казахстан) и Баку (Азербайджан).

VEKA Rus – дочерняя производственная компания концерна VEKA AG (Германия), одного из мировых лидеров в области разработки и производства оконных и дверных систем из высококачественного пластика. VEKA стала первой европейской экструзионной компанией, которая открыла в России собственный завод. Сегодня VEKA Rus имеет заводы, склады и представительства в нескольких городах России и других странах СНГ. Осенью 2017 года перед ИТ-департаментом компании встала задача по усилению безопасности оконечных устройств на протяжении всего жизненного цикла потенциальных угроз. Требовалось ускорить обнаружение кибератак и повысить эффективность ИБ-системы.

После анализа разработок, представленных на рынке, выбор был сделан в пользу оборудования Cisco. В числе преимуществ AMP for Endpoints – легкость внедрения, облачное управление, реализуемое по принципу «ПО как услуга» (SaaS), и возможность использования наряду с существующими антивирусными программами. Локальные средства защиты от вредоносного ПО – последний и часто единственный рубеж обороны для полностью зашифрованных каналов коммуникации, в том числе ведения архивов с парольной защитой, подключений HTTPS/SFTP, передачи файлов чата и т.п. Решение Cisco AMP анализирует все

файлы, попадающие в систему пользователя и блокирует вредоносное ПО на точке входа, тем самым устраняя необходимость в дорогостоящих технологиях для обеспечения безопасности конечных устройств.

Заведомо вредоносный файл сразу помещается в карантин. Редкие файлы – те, что не встречались ранее и не были зафиксированы в истории, – автоматически попадают в «песочницу» Threat Grid, которая осуществляет статический и динамический анализ. Таким образом действует ретроспективная защита: вредоносное ПО, не выявленное при первоначальной проверке, может быть обнаружено на этом этапе. Используя комбинацию файловых сигнатур, данные «песочницы», информацию о репутации файлов и поведенческих индикаторах, решение Cisco AMP for Endpoints способно блокировать выполнение исходного набора эксплойтов в пользовательской системе, а также предотвращать запуск загруженного файла программы-вымогателя или удалять его.

Кроме того, решение Cisco AMP непрерывно анализирует и записывает сведения об активности файлов в системе, независимо от их статуса. Если файл начинает проявлять подозрительную активность, Cisco AMP обнаруживает его и отправляет соответствующее оповещение администратору. Вместе с тем решение постоянно фиксирует подробную историю «поведения» вредоносного ПО, в том числе место и способ проникновения в сеть, пройденный путь и совершенные действия. Затем, на основе установленной политики, Cisco AMP помогает изолировать или устранить угрозу (автоматически или вручную).

Оборудование интегрируется с решением по контролю сетевого доступа с учетом контекста Cisco Identity Services Engine (ISE). В рамках единой платформы Cisco ISE включает в себя сервисы аутентификации, авторизации и учета (AAA), оценки состояния, профилирования и управления гостевым доступом. Согласованная работа продуктов позволяет обогащать контекст принятия решений в процессе авторизации в сети.

«Сегодня изоляция угроз на конечных устройствах наших сотрудников эффективнее, чем когда-либо, – говорит Сергей Токарев, заместитель руководителя отдела информационных технологий компании VEKA Rus. –

Киберпреступность стремительно развивается, и, предвосхищая попытки злоумышленников, мы укрепили границы с помощью решения Cisco AMP for Endpoints. В планах – аналогичное оснащение киевского офиса и закупка Cisco AMP для межсетевых экранов. Архитектурный подход к обеспечению информационной безопасности позволил нам усилить позиции за счет комбинации средств обнаружения, мониторинга и анализа».

«Решение AMP for Endpoints многофункционально, – рассказывает Гузель Мошнина, менеджер Cisco по продажам ИБ-решений. – Непрерывный мониторинг, ретроспективный анализ и интегрированная защита от угроз позволяют охватить весь период атаки: до начала, во время проведения и после завершения. Благодаря внедрению Cisco AMP for Endpoints в компании VEKA Rus значительно возросла скорость выявления возможных вторжений».

Метки: *Cisco AMP for Endpoints, Cisco Identity Services Engine (ISE), Cisco Threat Grid, информационная безопасность, защита данных.*

Пресс-служба Cisco в России/СНГ
Юлия Шведова
yshvedov@cisco.com

О компании Cisco

Cisco - мировой лидер в области информационных технологий, с 1984 способствующий развитию Интернета. Наши сотрудники, партнеры и разрабатываемые решения обеспечивают безопасные подключения, помогая воспользоваться преимуществами цифровых технологий будущего уже сегодня.

Узнать больше о решениях, технологиях и текущей деятельности компании можно на сайтах www.cisco.ru и www.cisco.com, а также в «Твиттере» @CiscoRussia.

Cisco, логотип Cisco, Cisco Systems и логотип Cisco Systems являются зарегистрированными торговыми знаками Cisco Systems, Inc. в США и некоторых других странах. Все прочие торговые знаки, упомянутые в настоящем документе, являются собственностью соответствующих владельцев.



О компании VEKA Rus

VEKA Rus - дочерняя компания международного концерна VEKA AG, специализирующегося на проектировании и производстве высокоэффективных оконных и дверных систем из специального высококачественного пластика. В России VEKA располагает двумя предприятиями в Москве и в Новосибирске. Продукция VEKA и ее партнеров позволяет существенно сократить расходы на отопление, сделать квартиру или дом по-настоящему комфортными и безопасными.

Подробнее с решениями VEKA вы можете ознакомиться на сайте <http://www.veka.ru/>, а также на наших страницах в Facebook и Вконтакте.

Смотрите нас на youtube: <https://m.youtube.com/user/OknaVEKARus>