Тысячи компаний в Беларуси готовы строить информационную безопасность в экосистеме Kaspersky

Дмитрий Кудревич, официальный представитель Kaspersky в Беларуси, — о том, почему на рынке информационной безопасности назрела необходимость в экосистемном подходе и почему при построении системы кибербезопасности важно учитывать отраслевую специфику

— Можно ли говорить о том, что организации в Беларуси стали чаще подвергаться кибератакам?

— Выросло количество целевых кибератак. Ряд отраслевых лидеров, национальных операторов инфраструктуры на протяжении последних нескольких лет были атакованы таким образом, что они теряли полный контроль над процессами: организациям был нанесён существенный урон. При этом еще в конце прошлого года наши специалисты неоднократно фиксировали целевые вредоносные рассылки, направленные на белорусские организации. Поэтому на всех уровнях сейчас уделяется пристальное внимание вопросам информационной безопасности. Частный бизнес значительно увеличил инвестиции в безопасность, чтобы не произошли события, которые могут его остановить или повлиять на инфраструктуру, критически важную для продолжения деятельности.

— Можете ли вы выделить конкретные типы угроз или атак, с которыми чаще всего сталкиваются предприятия в Беларуси?

— Если говорить о конкретных вредоносных программах, то вымогатели, шифровальщики, майнеры — всё это остается актуальным. Но важно понимать в первую очередь, почему атаки в принципе становятся возможны, даже если защита на уровне технологий выстроена на корректно. Часто роковую роль играет человеческий фактор, то есть сотрудники совершают — по незнанию или небрежности — ошибки, в результате которых злоумышленники получают возможность совершить кибератаку. Они пользуются недостаточным уровнем цифровой грамотности сотрудников и, например, применяют методы социальной инженерии, в том числе с использованием языковых моделей серии GPT-4, чтобы проникнуть в

корпоративную инфраструктуру. Бывает и так, что сотрудник становится инсайдером и осознанно воздействует на инфраструктуру предприятия, в котором он работает, по каким-то своим мотивам, например по финансовым.

— **Как развивается сейчас рынок решений для кибербезопасности?**

Логика развития рынка информационной безопасности сегодня так или иначе ведёт его к экосистемности. Экосистемный подход предполагает, что все продукты существуют в единой среде, максимально синхронизированы друг с другом и просты в управлении. Таким образом любые вопросы можно решить в режиме одного окна, для крупных корпоративных и промышленных инфраструктур система кибербезопасности становится более управляемой и, как следствие, более эффективной. Это позволяет анализировать и предвосхищать все возможные векторы атак, сокращая среднее время обнаружения инцидентов, реагирования на них и расследования, что в свою очередь позволяет экономить ресурсы организации и повышать её эффективность, упрощает работу ИТ-команды, высвобождает ресурсы для решения стратегических задач.

— Как именно Kaspersky реализует экосистемный подход?

Мы считаем, что у любой компании должна быть возможность настроить систему информационной безопасности под свои потребности и бюджет. Поэтому предлагаем рынку доступную, при этом, всеобъемлющую кибербезопасность. Она базируется на трёх китах. Первый — защищаем всех — от домашних пользователей до крупных корпораций и государственных органов. Второй — защищаем со всех сторон, то есть ограждаем все виды цифровых активов от всех возможных типов киберугроз. Третий — учитываем перспективы информационной безопасности в настоящем, то есть способствуем развитию индустрии сегодня с учётом тенденций будущего, активно вкладываемся в инновации и выходим за пределы традиционного представления о кибербезопасности.

Каждый из принципов мы воплотили в нашей линейке решений Kaspersky Symphony. Так, для малого и среднего бизнеса требуются оптимальные решения для автоматического обнаружения и нейтрализации как массовых, так и сложных угроз. Этот подход реализован в Kaspersky Symphony Security, которое обеспечивает фундаментальную безопасность всех рабочих мест — физических и виртуальных. Для тех организаций, которым сложно реализовать защиту рабочих мест от всех типов угроз и реагирование на инциденты своими силами, подойдет управляемая защита от MSSP партнера Kaspersky, подразумевающее передачу части функций ИБ сторонним специалистам. Представителям среднего и крупного сегмента, в распоряжении которых от 1000 до 3000 рабочих устройств, подойдут решения в сегменте детектирования и реагирования на инциденты, Endpoint Detection and Response – все необходимое есть в комплексе Kaspersky Optimum Security. А для критически важных объектов реального сектора экономики, которым требуется отражать сложные кибератаки и необходимо «экспертное» плечо в выборе персонализированной стратегии управления кибербезопасностью, подходит защита класса XDR (Extended Detection and Response).

— **Что есть в экосистеме Kaspersky, почему компании должны предпочесть ваши решения?**

Наша главная цель — решать проблемы кибербезопасности клиентов с учётом их отрасли, их болевых точек. Наш подход учитывает многообразие инфраструктуры и вложенные ранее инвестиции. Мы предоставляем широкий спектр решений, из которых заказчики могут выбрать те, которые помогут закрыть их точечные потребности. Мы предлагаем гибкость в выборе решения, ориентированного на конкретные задачи вертикалей управления.

Не будет преувеличением сказать, что мы являемся наиболее зрелым поставщиком в Беларуси, поскольку наш подход основан на 27-летнем опыте работы по всему миру и учитывает степень зрелости корпоративной безопасности. У нас есть комбинация продуктов, которая позволяет в рамках бюджета получать максимально эффективную защиту. Мы готовы предоставить защитные решения, позволяющие противостоять угрозам любого типа, чтобы любая компания могла настроить систему информационной безопасности под свои потребности и возможности. И лучшее подтверждение этому — тот факт, что нас уже выбрали тысячи ключевых организаций в Беларуси и сотни тысяч пользователей, у которых наши защитные решения стоят на личных смартфонах и ПК.