Круглый стол

Багхантинг как инструмент работы ИБ-служб

В круглом столе принимают участие

Олег БОСЕНКО,
директор департамента кибербезопасности компании IBS

Анатолий ИВАНОВ,
руководитель платформы Standoff Bug Bounty, компания Positive Technologies

Елена МОЛЧАНОВА,
бизнес-лидер киберполигона Standoff, компания Positive Technologies

Никита РАСПОПОВ,
специалист по анализу защищенности компании УЦСБ

Михаил СУХОВ,
руководитель отдела анализа защищенности компании Angara Security

В настоящее время наличие багбаунти-программы – правило хорошего тона для крупного бизнеса либо естественное продолжение регулярного проведения таких работ, как пентест или редтиминг. Это подтверждается ростом количества программ со стороны не только ИТ-гигантов, но и Правительства. Можно ли считать багхантинг инструментом работы служб ИБ крупных отечественных предприятий, и насколько он универсален?

Широко ли распространен багхантинг в качестве инструмента работы служб ИБ крупных отечественных предприятий? Насколько он универсален и применим к большинству предприятий крупного бизнеса?

Анатолий ИВАНОВ:

Подход багбаунти вытесняет пентесты, потому что рынок предложений пентестов перестал справляться со спросом. Пентесты сейчас делают все, кому не лень, в том числе студенты и новички. Из-за этого качество услуги снижается, и компании выходят на платформы багбаунти. Такой подход удобен всем, кто раньше заказывал пентесты.

Никита РАСПОПОВ:

Количество багбаунти-программ, реализуемых крупным бизнесом, продолжает увеличиваться. Главное отличие багбаунти от пентеста или редтима заключается в отсутствии ограничений по времени и привлечении большего количества специалистов. На сегодняшний день поддержка такой программы требует со стороны компании наличия ИБ-отдела с соответствующими компетенциями и выстроенными процессами. Это нужно, чтобы компания могла эффективно проводить оценку полученных отчетов и устранять уязвимости. Обычно такие ресурсы есть у крупного бизнеса, так как в связи с высокой актуальностью рисков ИБ наличие грамотного ИБ-отдела и соответствующего бюджета в наше время стало необходимостью.

Михаил СУХОВ:

В последние годы отечественные компании, в том числе государственные, все чаще открывают

программы багбаунти. Это связано преимущественно с тем фактом, что в 2022 г. для российских компаний была закрыта самая большая международная платформа для взаимодействия между «белыми» хакерами и представителями компаний, что привело к развитию отечественных платформ.

Но, к сожалению, не всем компаниям подходит подобный процесс поиска уязвимостей. Ведь создание и поддержка таких программ требуют компетенций и ресурсов, причем не только экономических, для оценки отчетов, общения с «белыми» хакерами и т. д. Поэтому не всем компаниям подходят программы багбаунти, для этого требуются зрелые процессы информационной безопасности. И ключевой из них – процесс управления уязвимостями. Для него необходимы не только компетенции по ИБ, но и правильно выстроенный процесс взаимодействия с ИТ-департаментом.

В какой степени удалось заместить иностранные платформы багбаунти отечественными? Насколько они сопоставимы по функциональности, надежности и производительности?

Анатолий ИВАНОВ:

Российские платформы багбаунти полностью заменили иностранные. Компании, которые выходили на Standoff Bug Bounty после hackerone, отмечают, что за день им пришло больше отчетов, чем за месяц на иностранной площадке.

Поскольку наши коллеги раньше работали с иностранными площадками, то столкнулись с проблемой некачественного триажа (разбора отчетов экспертами площадки). Пришлось самим выстраивать соответствующий процесс.

Никита РАСПОПОВ:

В настоящее время отечественные платформы набирают обороты. Еще три года назад основной платформой для багбаунти были HackerOne или BugCrowd. Сейчас у нас собственные площадки, на которых представлены передовые компании. Среди их достоинств можно выделить наличие крупного бизнеса и государственных информационных систем на багбаунти-платформах.

Развитие отечественных платформ служит, в частности, инструментом для повышения компетенций исследователей, что, в свою очередь, помогает быстрее обнаруживать и устранять уязвимости. Кроме того, участие государственного сектора дает сигнал о признании багбаунти со стороны государства, что расширяет потенциал развития в этой сфере.

Сегодня актуальна проблема повышения качества взаимодействия со службами поддержки отечественных багбаунти-платформ, в том числе по вопросам, затрагивающим взаимодействие вендоров и багхантеров. Устранение различных препятствий – это вопрос времени и естественного развития багбаунти-платформ.

Михаил СУХОВ:

Стоит отметить основное отличие – интеграцию с российским законодательством и налогообложением. Например, у одной отечественной платформы выплата занимает три дня. Это сильный прогресс по сравнению с иностранной платформой. В целом отечественные платформы создали хорошую альтернативу иностранным площадкам.

Каковы основные тренды отечественного рынка услуг управления уязвимостями? В каком направлении, на ваш взгляд, пойдет его развитие в ближайшей перспективе?

Олег БОСЕНКО:

В качестве трендов отечественного рынка услуг управления уязвимостями можно выделить внедрение процедур выявления уязвимостей и управления процессом их устранения, а также расширение периметра применения безопасной разработки программного обеспечения или DevSecOps разработчиками программного обеспечения. Требование безопасной разработки все чаще указывается в документации на закупки и в требованиях к программным продуктам.

При этом следует учитывать одну важную особенность – чем больше в программном продукте Open source, тем больше уязвимостей можно получить на старте. Взаимосвязь крайне простая: снизилась внутренняя дисциплина программирования, большое количество разработок отправляются в библиотеки без должной проверки, не исключено умышленное наличие уязвимостей в Open source от определенного круга разработчиков из целого ряда государств. Соответственно, выявление уязвимостей возможно только на следующих шагах. К сожалению, нельзя спрогнозировать их количество, еще до начала адаптации программного продукта нужно определиться с уязвимостями.

Михаил СУХОВ:

Основной тренд – аутсорс – относится не только к информационной

безопасности и тем более не только к процессу управления уязвимостями. Его формирование объясняется нехваткой компетенций и ресурсов на рынке труда в текущий момент. По этой причине все чаще даже крупные компании смотрят в сторону аутсорса ресурсов для построения процессов. В ближайшем будущем ожидается развитие услуг по сканированию уязвимостей внешнего периметра и внутренней инфраструктуры компании.

Для предоставления таких услуг важно привлечь высококвалифицированных специалистов, погруженных в актуальные тренды в сфере уязвимостей и разрабатывающих собственные инструменты для поиска и отслеживания уязвимостей. Получение компанией только актуальной, подтвержденной и торпедированной по критичности информации существенно улучшает и облегчает первый этап процесса управления уязвимостями.

Как вы оцениваете текущий уровень открытости взаимодействия отечественных ИТ-разработчиков и ИБ-исследователей в сфере обнаружения и дальнейшего устранения уязвимостей?

Олег БОСЕНКО:

Уровень открытости можно оценить как хороший, уровень взаимодействия – как недостаточный, уровень открытости взаимодействия – как низкий. Обсуждение вопросов уязвимостей и безопасной разработки программного обеспечения продолжается на различных площадках под эгидой госструктур, а также на коммерческих площадках. И это уже не тенденция, а устоявшийся процесс.

Взаимодействие между составляющими процесса (ИТ и ИБ) пока только выстраивается, что объясняется несколькими причинами. Основная – уязвимости и работа по ним рассматриваются в сообществе как задачи информационной безопасности, хотя отделять процесс от ИТ крайне ошибочно. Сохраняется еще и нежелание разработчиков «подсвечивать» наличие уязвимостей в разрабатываемых продуктах. От этого и уровень открытости взаимодействия страдает.

Никита РАСПОПОВ:

На сегодняшний день ИТ-разработчиков можно разделить на два вида. Первый – реагирует конструктивно и идет навстречу в совместном устранении и раскрытии уязвимостей. Разработчики повышают уровень безопасности, а исследователь получает возможность зарегистрировать уязвимость и рассказать о ней сообществу. Такие вендоры – пример высокого уровня открытости и зрелости.

Второй вид вендоров, к сожалению, реагирует негативно, пытаясь доказать, что «это не баг, а фича». В результате диалог либо прекращается, либо вовсе не начинается. Хотелось бы, чтобы доля влияния ИТ-разработчиков первого вида росла более быстрыми темпами, поскольку нехватка открытости в коммуникациях приводит, прежде всего, к уязвимостям в инфраструктурах организаций.

Как вы оцениваете перспективы развития киберполигонов в России? Насколько оправдан тренд на отраслевую кастомизацию?

Олег БОСЕНКО:

Перспективы развития киберполигонов есть. Это одно из современных направлений подготовки ИБ к противодействию атакам. Вместе с тем стоит отделять реальную подготовку к противодействию (когда киберполигон является площадкой отработки действий, тренировки персонала, проверки алгоритмов СУИБ) от «хайпа» различных трешбитв и соревнований в ходе конференций, форумов и т. д. Вторая часть к реальной безопасности отношения не имеет: это спорт века высоких технологий, а не системная безопасность.

Что касается отраслевой кастомизации, то она оправдана. В первую очередь это связано с характером объектов (площадные, линейные, территориально распределенные, ОКИИ, ЗОКИИ), набором информационных решений и особенностями информационных и производственных процессов.

Елена МОЛЧАНОВА:

Киберполигоны и киберучения, которые на полигонах обычно и проводятся, действительно крайне востребованы сегодня. Компании сталкиваются со все возрастающим числом и сложностью атак, и чтобы успевать справляться с вызовами, надо нарабатывать опыт столкновения с ними. Но опыт желательно получать так, чтобы не ставить под угрозу собственную инфраструктуру. Такую возможность и дает полигон.

Для начала мы рекомендуем учиться на типовых инфраструктурах, характерных для конкретной отрасли: они максимально приближены к реальной жизни (реальные ПО, оборудование, бизнес-процессы, риски). Приступать к работе на полигоне можно почти сразу. А затем можно кастомизировать полигон под конкретную специфику – вплоть до учений на вашем цифровом двойнике. ■