что ждет нас в будущем: угрозы безопасности в 2015 году

В 2015 году исполняется 30 лет двум ключевым публикациям в сфере информационной безопасности — *The Hackers Handbook* в Великобритании и первому выпуску журнала *Phrack* в США. Оба издания стали историческими, они содержали подробные инструкции о том, как внедриться в компьютерные системы и управлять ими — и это в год, когда только поступил в продажу первая версия Microsoft Windows.

За прошедшие годы мир информационных технологий изменился до неузнаваемости, и ландшафт информационных угроз вместе с ним. Мы спросили нескольких специалистов по информационной безопасности, какие критические тенденции будут наблюдаться в наступившем году в этой сфере.

1. получит широкое распространение информационный рэкет предприятий

Конец 2014 года ознаменовался масштабной и грязной атакой на компанию Sony. Злоумышленники взломали ее информационные системы и угрожали опубликовать данные в случае, если их требования не будут удовлетворены. Джейсон Вуд (Jason Wood), генеральный консультант по безопасности фирмы Secure Ideas, занимающейся обеспечением информационной безопасности, считает, что в 2015 году количество подобных атак только возрастет.

Пользователи сталкиваются с атаками с требованием выкупа вот уже несколько лет. Злоумышленники вымогают деньги за возвращение доступа к зашифрованным данным. Информационный рэкет на уровне корпораций будет встречаться все чаще, предупреждает Вуд.

«Крупномасштабное уничтожение ресурсов отмечалось уже несколько раз, и в будущем, вероятно, получит еще более широкое распространение. Возможно, злоумышленники действительно смогут наживаться на захваченных данных и системах предприятий».

2. станет стандартом двухфакторная проверка подлинности (2FA)

Эпоха паролей еще не закончилась, но, по мнению экспертов, в 2015 году нормой станут альтернативные механизмы. «Нам необходимо перейти от паролей к чему-то другому. Вспомните хотя бы о LinkedIn и случившейся с ними утечке», — предупреждает Джамаль Элмеллас (Jamal Elmellas), технический директор Auriga, консалтинговой фирмы в сфере компьютерной безопасности. Он имеет в виду массовую утечку данных в 2012 году, когда в открытый доступ попали 6,5 млн похищенных паролей LinkedIn.

Неэффективное управление паролями означает, что не менее 60% паролей, хранящихся в виде хэш-суммы, можно раскрыть методом перебора за несколько дней. «Кто-то получает доступ к базе данных и обнаруживает, что в ней используются слабые алгоритмы шифрования и хэширования. А кто-то проникает в базу паролей… Угадаете, что будет дальше? Все мы люди и часто используем одинаковые пароли на разных ресурсах».

Джон Пескаторе (John Pescatore), директор по вопросам новых тенденций в безопасности SANS Institute, уточняет, что новые механизмы развиваются все интенсивнее. До недавнего времени, объясняет эксперт, пользователи неохотно применяли любые методы проверки подлинности, за исключением повторяющихся паролей.

«В конце концов настал переломный момент. Теперь пользователи думают: "Проще воспользоваться механизмом аутентификации Google, с получением SMS, чем снова менять все номера кредитных карт"».

Эти изменения уже отразились на потребительских приложениях, и теперь, по мнению эксперта, новые тенденции проявятся и в корпоративном секторе. На недавнем семинаре SANS, посвященном проблемам в сфере обеспечения безопасности систем здравоохранения, некоторые компании объявили о начале тестирования методов двухфакторной верификации с использованием телефонов.

3. вектором атаки станут системы M2M

Угрозе будут подвержены не только пароли и данные, считает доктор Адитья Суд (Aditya Sood), соавтор книги *Targeted Cyber Attacks* («Целенаправленные кибератаки»). Потенциальную опасность будут представлять самые неожиданные устройства, поскольку подключенные к интернету сенсоры станут распространенным вектором атаки.

«Станут популярными такие методы атаки, как злонамеренное и неправомерное применение интернета вещей (IoT) для осуществления атак через цифровые устройства», — поясняет эксперт. Он считает, что данная тенденция осложнит сбор полезных данных для анализа и обработки.

Системы диспетчерского контроля и сбора данных (SCADA) также будут высокоприоритетными целями, поскольку они позволяют управлять критически важными операциями, предупреждает Суд. Совсем недавно Майкл Роджерс (Michael Rogers), адмирал штаба интернет-операций ВС США и директор Агентства национальной безопасности, заявил, что ряд стран обладает достаточными возможностями для осуществления кибератак, способных вызвать отключение компонентов сети электроснабжения США.

4. обязательной мерой станет проверка программного обеспечения

Эксперты считают, что следует ожидать роста активности по поиску уязвимостей в широко распространенном программном обеспечении, поэтому возможность подтверждения безопасности ПО станет очень важной.

2014 год ознаменовался обнаружением Heartbleed и Shellshock, крайне опасных наборов ошибок в широко распространенном открытом ПО. Эти угрозы сказались на множестве интернет-систем. Суд считает, что в 2015 году злоумышленники будут уделять все больше внимания критически важному ПО, поскольку оно широко используется в различных подключенных к интернету системах. «Это станет закономерностью, поскольку обнаружение проблемы безопасности в критически важном программном обеспечении значительно затронет весь интернет», — объясняет он.

Этот и другие факторы приведут к появлению систем проверки подлинности ПО в наступившем году. Мы предполагаем, что в условиях, когда компании подозревают наличие в ПО (включая встроенное) интегрированных способов обхода систем защиты, на первый план выйдет требование проверки отсутствия уязвимостей в ПО.

«Еще одна тенденция: всем производителям программного обеспечения придется доказывать, что их продуктам можно доверять и что в них отсутствуют встроенные механизмы обхода систем защиты. Это уже происходит», — утверждает Пескаторе. К примеру, китайский производитель программного обеспечения NSFocus привлек к проверке безопасности своих продуктов компанию Veracode, которая занимается поиском уязвимостей в приложениях других производителей.

5. появится новая мишень — мобильные системы

Состоящие из смартфонов ботнеты будут ориентированы практически исключительно на системы Android, предупреждает Суд. «Ботнеты будут создаваться или дорабатываться одновременно для мобильных устройств и стандартных компьютерных систем, — утверждает эксперт. — Мобильные устройства на платформе Android в новом году станут для злоумышленников приоритетной целью: они проще с точки зрения использования уязвимостей и извлечения данных».

Мобильные сетевые устройства превратятся еще в одну мишень, предупреждает Пескаторе. Мобильные беспроводные точки доступа, предназначенные для подключения устройств с поддержкой Wi-Fi к мобильным сетям, в 2015 году станут, по его мнению, критическим вектором атаки, поскольку они позволяют обходить брандмауэры предприятий.

«Люди имеют склонность обходить URL-фильтры, которые их как-либо ограничивают. В один прекрасный день в вашей компании может появиться несанкционированная точка доступа Wi-Fi, не фильтруемая брандмауэром, — говорит он. — Меня серьезно беспокоит такая возможность: администратор облачного центра данных решит оставить свой адаптер Wi-Fi в центре данных, чтобы на выходных управлять сервером удаленно».

Как лучше всего защититься от подобных угроз? Обычным способом: разумно сочетая учебные мероприятия для пользователей, современные версии технологических решений и внедрение эффективных процессов обеспечения безопасности. В комплексе эти меры создадут несколько уровней защиты. Однако еще важнее не обеспечивать безопасность в последний момент, а продумывать защитные меры заранее. Информационная защита должна лежать в основе всех действий организации, а не служить косметическими мерами.

Узнайте больше о решениях для обеспечения безопасности от Orange Business Services и познакомьтесь с возможностями решения Orange CyberSOC, которые помогут защитить вашу организацию от многих из перечисленных угроз.