ОТБИТЬ АТАКУ

ИНТЕНСИВНАЯ ЦИФРОВИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ ВО ВСЕХ СФЕРАХ ЭКОНОМИКИ ОБОСТРИЛА ПРОБЛЕМУ КИБЕРБЕЗОПАСНОСТИ: ХАКЕРЫ СТРЕМЯТСЯ ПОЛУЧИТЬ ДОСТУП К ФИНАНСАМ, ТЕХНОЛОГИЯМ И КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ КОМПАНИЙ. ЭКСПЕРТЫ ОБРАЩАЮТ ВНИМАНИЕ НА ТО, ЧТО КОЛИЧЕСТВО ХАКЕРСКИХ АТАК НА БИЗНЕС БЫСТРО РАСТЕТ, А ИНСТРУМЕНТЫ ЗЛОУМЫШЛЕННИКОВ СОВЕРШЕНСТВУЮТСЯ ВМЕСТЕ С ЦИФРОВЫМ РАЗВИТИЕМ. ДМИТРИЙ МАТВЕЕВ

ЕВГЕНИЙ ПАВЛЕНКО

ХАКЕРЫ АТАКУЮТ ОРГАНИЗАЦИИ ПО ВСЕМУ МИРУ КАЖДЫЕ 39 СЕКУНД, 2,244 ТЫС. РАЗ В ДЕНЬ, НО БОЛЬШАЯ ЧАСТЬ ТАКИХ АТАК НЕ ДОСТИГАЕТ ЦЕЛИ

По данным отчета Microsoft за 2019 год, 39% российских предприятий малого и среднего бизнеса сталкивались с целенаправленными атаками, а с массовым переходом на удаленную работу кибератаки стали еще более изощренными, говорит руководитель программ информационной безопасности Microsoft в Центральной и Восточной Европе Артем Синицын. С октября 2019 года по июль 2020 года наиболее частой причиной реагирования на инциденты стали программы-вымогатели, но не теряет своей популярности и фишинг: около 70% всех киберинцидентов пришлось на данный вид мошенничества. Среди новых видов угроз, указывает эксперт,— атаки на цепочки поставки и устройства IoT, в частности, на конечные точки интернета вещей: в первом полугодии 2020 года число таких атак выросло на 35%.

В течение последних двух-трех лет число атак действительно неизменно увеличивается от квартала к кварталу, солидарен с представителем Microsoft директор экспертного центра безопасности Positive Technologies Алексей Новиков: по итогам второго квартала 2020 года показатель вырос на 9% по сравнению с первым кварталом и на 59% по сравнению с аналогичным периодом прошлого года. «Любое громкое мировое событие неминуемо сопровождается ростом числа кибератак, поскольку они создают благоприятную почву для применения злоумышленниками методов социальной инженерии. Так, апрель и май 2020 года стали рекордными по числу успешных кибератак, в том числе использующих тематику эпидемии, а также ориентированных на нюансы авральной диджитализации бизнеса, которая зачастую проходила без учета требований безопасности»,— отмечает он.

Ведущий системный инженер компании Varonis Александр Ветколь обращает внимание на то, что хакеры атакуют организации по всему миру каждые 39 секунд, 2,244 тыс. раз в день, но большая часть таких атак не достигает цели. По подсчетам центра мониторинга и реагирования на кибератаки Solar JSOC, в России в 2018 году совершено 765 тыс. атак, а в 2019 году — уже более 1 млн, говорит инженер по безопасности REG.RU Артем Мышенков, при этом в разгар пандемии коронавируса количество атак увеличилось в пять раз, в том числе из-за удаленной работы. Директор по внешним связям в Восточной Европе и Средней Азии координационного центра RIPE NCC Максим Буртиков приводит альтернативные статистики: по данным компании «Ростелеком-Солар», за 2019 год попытки взлома фиксировались на 30% чаще, доля внешних инцидентов выросла с 54 до 58%, по данным же Cybersecurity Ventures, попытки мошенничества совершались раз в 14 секунд.

С переходом на удаленную работу количество инцидентов информационной безопасности растет, соглашается с коллегами руководитель департамента IT-решений и продуктов информационной безопасности компании «Билайн Бизнес» Александр Пономарев: «цифровая гигиена» в России пока еще недостаточно развита. «Сейчас набирают популярность подготовленные атаки на бизнес, целью которых является как кража денег или конфиденциальной информации в рамках промышленного шпионажа, так и причинение репутационного ущерба. Иногда просто переход по ссылке в браузере корпоративного компьютера запускает очень опасные процессы, цена которых измеряется шестизначными цифрами и может устраняться несколько месяцев»,— говорит он.

Руководитель направления внедрения и поддержки корпоративных решений компании Sharesoft Константин Замков напоминает, что ежегодно в публичных источниках появляются сведения о сотнях случаев утечки данных из российских компаний, а по количеству утечек РФ занимает второе место в мире после США, и чаще всего в них виновны сотрудники компании, лишь менее одной пятой части утечек происходит из-за хакеров.

ШИРОКИЙ КРУГ ИНТЕРЕСОВ Раньше основной целью самых опасных атак были преимущественно финансовые организации, поскольку главной мотивацией хакерских групп являлась прямая финансовая выгода, рассказывает руководитель центра мониторинга и реагирования на инциденты информационной безопасности Jet CSIRT Алексей Мальнев, однако все чаще целью кибератак является информация, которую можно монетизировать лишь косвенно, а постепенная трансформация организаций буквально всех отраслей в IT-компании делает их равнозначной целью: неважно, идет ли речь о системах управления инфраструктурой в медицинских учреждениях, в логистических и транспортных компаниях или химической промышленности, так как шифровальщики могут парализовать любой бизнес.

Генеральный директор ООО «Доктор Веб» Борис Шаров отмечает, что его компания чаще всего сталкивается с атаками, проводимыми против госкомпаний и крупных коммерческих структур, при этом профиль не важен, принцип один: атакуемая организация должна представлять определенный финансовый интерес для атакующего. По словам Александра Ветколя, наибольшие потери от атак в 2019 году — $25 млрд — фиксировались у медицинских организаций.

По данным Positive Technologies, распределение категорий «жертв» среди юридических лиц по итогам первого полугодия такое: госучреждения — 16%, промышленность — 15%, торговля — 7%, медучреждения, финансовые организации и IT-компании — по 6%. Традиционно атакам наиболее часто подвергаются финансовый, государственный и промышленный сектора, соглашается с коллегами директор департамента информационных технологий Accent Capital Иван Мельник, а меры противодействия могут быть самые разные: защита периметра, шифрование хранящихся данных, проведение penetration-тестов и устранение выявленных уязвимостей, антивирусная защита, повышение осведомленности персонала.

Бизнес-консультант по безопасности Cisco Алексей Лукацкий в качестве примера крупных хакерских атак приводит несколько инцидентов: компания Garmin пострадала от атаки вымогательского ПО, и многие ее системы оказались зашифрованными; морской перевозчик Maersk столкнулся с шифровальщиком NotPetya (Neytya), в результате чего встали многие перевозки по всему миру на несколько недель, а в результате взлома Sony в 2014 году были украдены не только персональные данные сотрудников и данные о доходах руководства компании, но и релизы еще не вышедших фильмов, планы по новым картинам и их сценарии. «Хакеры зарабатывают на своей деятельности доходы, сопоставимые с торговлей оружием, наркотиками и алкоголем»,— подчеркивает он.

СКРЫТАЯ УГРОЗА Чаще всего компании не замечают наличие атаки, поскольку хакеры становятся хитрее и прорабатывают многоэтапные атаки длительностью до нескольких лет, говорит генеральный директор компании Omega Алексей Рыбаков. В таких случаях подключение ведется чаще всего через партнеров или поставщиков компании-объекта атаки, с которыми налажены доверительные информационные каналы. «Если проанализировать, насколько быстро крупные промышленные или энергетические компании с их киберзащитой и закрытостью могут выходить из строя, логично предположить, что защита многих из них уже взломана, но программа взлома находится в спящем режиме, и для завершения атаки с реальными послед-