12+

Джимшер Челидзе

{ ЦИФРОВАЯ ТРАНСФОРМАЦИЯ для директоров и собственников

часть 3 КИБЕРБЕЗОПАСНОСТЬ }

Джимшер Челидзе

Цифровая трансформация для директоров и собственников. Часть 3. Кибербезопасность. Часть 3. Кибербезопасность

«Издательские решения»

Челидзе Д. Б.

Цифровая трансформация для директоров и собственников. Часть 3. Кибербезопасность. Часть 3. Кибербезопасность / Д. Б. Челидзе — «Издательские решения»,

ISBN 978-5-00-604654-2

Эта небольшая книга вмещает в себя много материала об информационной безопасности, изобилует статистикой, примерами и деньгами. В книге даны пошаговые рекомендации по защите компании от киберугроз.Как и в предыдущих частях о цифровизации, я фокусируюсь на системном подходе, избегая классической ошибки — фокуса на технологиях и ожидания чуда от них. В книге показано, как ИБ связана с процессами, компетенциями, внутренней коммуникацией, бережливым производством и управлением проектами.

ISBN 978-5-00-604654-2

Содержание

Цифровая трансформация для директоров и собственников. Часть 3. Кибербезопасность
Часть 3. Кибербезопасность

Джимшер Бухутьевич Челидзе

Редактор Александр Александрович Перемышлин
Дизайнер обложки Александр Александрович Перемышлин
Иллюстратор Александр Александрович Перемышлин

ISBN 978-5-0060-4654-2
Создано в интеллектуальной издательской системе Ridero

Предисловие

Здравствуй, дорогой читатель. Это заключительная книга про цифровизацию и цифровую трансформацию. В первой книге мы разобрали, что такое цифровизация и цифровая трансформация, зачем они нужны, в чем разница, какие есть подводные камни. Во второй познакомились с системным подходом, который применим не только для цифровой трансформации, но и в целом для любого бизнеса. Системный подход сочетает проверенные инструменты и цифровизацию, доступен любому и призван повысить отдачу от цифровых технологий, а также минимизировать риски, связанные с организацией работы. При этом, еще в первой части мы проговорили, что в ролевой модели для цифровой трансформации необходим специалист по информационной безопасности. И именно этому направлению я решил посвятить отдельную книгу.

Казалось бы, цифровизация и кибербез несовместимы, но без того, чтобы их подружить, невозможно продолжать цифровизацию. Недавно у Дениса Батранкова я встретил хорошее определение, почему же нужно заниматься информационной безопасностью сейчас: «Раньше безопасность была построена на истории про акулу: не надо быть впереди всех уплывающих от нее – достаточно быть впереди последнего. А вот сейчас, когда целью акулы являешься именно ты – защищаться стало сложнее». И это определение крайне точно описывает текущую ситуацию, так как с каждым годом атаки хакеров становятся все более адресными. А 2022 год вообще стал знаковым.

Этой книги не было бы без исследований Positive Technology (далее – PT), ставших первыми моими проводниками в мир кибербезопасности. И если вы любите досконально погружаться в первоисточники, детали, то рекомендую изучить эти исследования. QR-коды и ссылки на них будут в конце книги.

Книга состоит из трех частей. Первая посвящена обзору и анализу текущей ситуации. Будет много цифр, статистики, аналитики, денег. Задача первой части – сформировать у вас осознание проблемы и понимание того, что информационная безопасность (далее – ИБ) – направление столь же стратегическое, как и вся цифровизация, и она достойна вашего внимания. Главный тезис обозначу сразу – узкое место в безопасности, как и во всей цифровизации, – процессы и люди, не только ваши, но и в команде разработчиков программного обеспечения (далее – ПО).

Вторая часть посвящена интеграции информационной безопасности с точки зрения системного подхода.

Ну, а третья часть посвящена практическим рекомендациям, что делать здесь и сейчас, как выбирать ИТ-решения для информационной безопасности, что необходимо знать людям и какие нужны компетенции.

Если вы читали предыдущие книги, то уже знаете мой подход – чтобы кого-то контролировать и делегировать задачи, доверять своей команде, нужно хотя бы базово понимать ее работу. И ключевая задача всей книги – дать вам базовые знания для выстраивания эффективной работы со своей командой и директором по ИБ (далее – CISO) с наименьшими трудозатратами и рисками для вас.

Также, чтобы исключить возможное недопонимание, давайте разберем, в чем разница между информационной безопасностью и кибербезопасностью?

Информационная безопасность – это деятельность, которая связана с предотвращением несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.

Кибербезопасность – все то же самое, только связанное с ИТ-системами и компьютерами.

Часть 1. Зачем заниматься информационной и кибербезопасностью?

Глава 1. Погружение и про деньги

В 2023 году уже очевидно, что без использования цифровых технологий невозможно ни вести бизнес, ни комфортно жить, ни управлять государством.

Если говорить про государственные сервисы, то госуслуги в виде онлайн-сервисов развиваются по всему миру. Россия же здесь вообще в числе мировых лидеров. Я, например, использую цифровые сервисы государства и для записи ребенка к врачу, и для просмотра его прививок с результатами анализов, и для оплаты штрафов, налогов, отправки налоговых деклараций.

Если говорить про коммерческий сектор, то он вообще без онлайн уже не может: оплата товаров, бронирование билетов, получение услуг, консультаций, появление цифровых советников.

В общем и целом, цифровизация и автоматизация всюду. И если их игнорировать, то вы будете просто неконкурентоспособными. А если хотите понять, что примерно нас ожидает через 5—10 лет, то рекомендую почитать наблюдения Евгения Бажова о том, что происходит в Китае, в его книге «Made in China. Как вести онлайн-бизнес по-китайски».

Давайте еще, для примера, коснемся работы с кадрами. Без облачных технологий и гибридного / удаленного режима работы вам будет намного сложнее привлекать талантливых сотрудников и/или будете значительно за них переплачивать. Да, рынок труда, конечно, меняется, и сейчас вновь работодатель начинает диктовать среднему работнику свои условия. Но это про средних работников. А если вы хотите привлекать таланты, то удаленка является мощным преимуществом. По моим личным наблюдениям удаленка/гибрид позволяет сэкономить на фонде оплаты труда до 30—40%. Молодые, гибкие, голодные до успеха компании этим активно пользуются. И в вакансиях я встречаю одну тенденцию: те, кто хотят меньше платить, просто дают возможность удаленной работы. Конечно, подробную статистику по срокам закрытия этих вакансий я не веду, но закрываются они быстро. Кажется, что даже быстрее, чем у компаний с более высокими зарплатами, но требованием ежедневно присутствовать в офисе.

Казалось бы, вот оно счастье – цифровизация. Но там, где появляются возможности, возникают и риски. Так, например, развитие удаленки в ковидный 2020 год привело к росту взломов мессенджеров и систем коллективных конференций. И ладно, если б просто подключались и портили онлайн-собрания, но у хакеров появилась другая тактика – они копируют конфиденциальные записи встреч и чатов, чтобы потом заниматься вымогательством. Еще один современный тренд – шифрование внутренних файлов с целью последующего выкупа.

Также необходимо посмотреть на небольших разработчиков ИТ-продуктов: сами по себе они могут быть никому не интересны, однако их могут атаковать для того, чтобы встроить в их продукт вредоносное ПО, и уже через него атаковать крупную компанию. И реализовать такой сценарий можно, даже не атакуя ИТ-инфраструктуру – нужно лишь завербовать удаленного сотрудника, который сам внесет нужные изменения в код. Такой подход, когда большие компании атакуются через подрядчиков и поставщиков, называется «атакой на цепочку поставок». Это еще один из главных трендов, начиная с 2021 года. В 2022 году до 30% целенаправленных атак приходилось на эту тактику.

Рисков тут добавляют и рост сложности ИТ-решений, и снижение квалификации среднего разработчика, ведь чем дешевле разработчик, тем выгоднее все с точки зрения экономики. Конкуренция и рынок хотят комплексных решений по минимальной цене, что обязывает

искать способы снизить стоимость продукта. Но в итоге все это ведет к увеличению количества дыр в ИТ-решениях. И вам угрожают не только прямые финансовые и юридические риски, связанные со штрафными санкциями от поставщиков и государства и с уголовной ответственностью, но и репутационный ущерб. А если вы вышли на биржу, то это еще и риски падения капитализации.

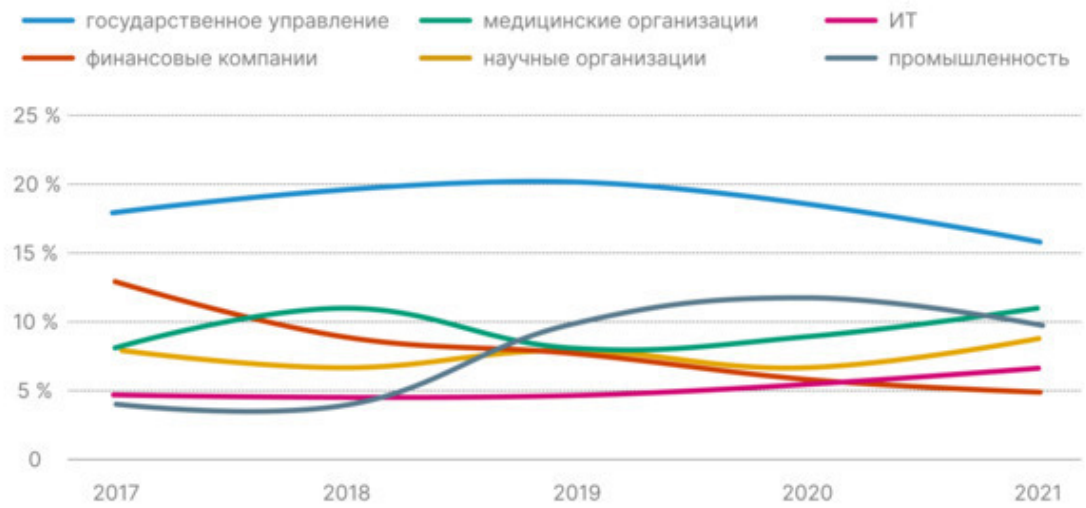
Наиболее яркий пример этого – атака на компанию SolarWinds. Их клиентами были правительственные учреждения США и более 400 крупнейших американских компаний. Хакеры внедрили вирус в их решение и атаковали их клиентов. Результат – падение стоимости акций на 40% за несколько недель.

Если же посмотреть на абсолютные числа, то с начала 2017 по конец 2022 года количество зафиксированных атак увеличилось с 985 до 2921, то есть рост составил 196,5%. Тут, конечно, надо учитывать и то, что научились лучше выявлять атаки, но, забегая вперед, скажу, что даже сейчас в 70% исследованных компаний выявлены вирусы, о которых и не знали. При этом количество целевых атак увеличилось с 43% в 2017 году, до 67% в 2022. И несмотря на то, что в 2021 году целевых атак было 73%, вероятность целевой атаки высока. Ведь 2022 год – год войны в киберпространстве, настоящая и широкомасштабная.

Теперь про деньги. Средняя стоимость выкупа, которую компании платят хакерам, также растет. Если раньше ограничивались условными 1—2 тысячами долларов, то сейчас это 4,35 млн. То же самое касается и максимальной выплаты. В 2017 году она составляла 1 млн долларов, в 2022 – уже более 40 млн.

Прогнозы тоже пессимистичны. Так Cybersecurity Ventures ожидает, что глобальные издержки от информационных атак будут расти на 15% и к 2025 году достигнут по всему миру 10,5 трлн долларов США в год, при 6 трлн в 2021 году и 3 трлн в 2015.

Также приведу график от PT того, как изменяются атаки, на кого нападали чаще, и кто сейчас стал пользоваться спросом у хакеров.



Динамика по отраслям, % от общего числа атак

Тут я рекомендую обратить внимание на финансовые компании – они все менее интересны, поскольку становятся все более сложными для атак. В целом же рынок «гражданского» хакерства все больше подчиняется законам бизнеса: злоумышленники ищут, как снизить стоимость каждой атаки и увеличить ее доходность. То есть хакеры ищут маржинальность. Но это касается только тех хакеров, которые не занимаются политическими заказами или целенаправленными атаками, например, от конкурентов. В итоге, с учетом того, что идет рост в сторону

от массовых атак к таргетированным, уповать на одну экономическую целесообразность атаки не стоит. Если вас закажут, то вы будете атакованы. Особенно если вы – российская компания. А если вы – первое лицо, то именно вы под прицелом в первую очередь.

Глава 2. Про ответственность

Сейчас ответственность за информационную безопасность несет руководитель организации, что отражено в указе президента Российской Федерации В. В. Путина от 01.05.2022 №250. Под его действие попадают федеральные органы исполнительной власти (федеральные министерства, службы и агентства), руководство субъектов РФ, государственные фонды, государственные корпорации и компании (например, «Росатом», «Газпром», «Русгидро», «РЖД» и другие), стратегические и системообразующие предприятия, объекты критической инфраструктуры.

И если на 20 апреля 2020 года в перечень системообразующих организаций входило 646 юридических лиц, то к июлю 2020 года их уже было около 1300, а в феврале 2022 – около 1400. Но, казалось бы, если вы не попадаете в этот список, то зачем он вам? Тут надо понимать, что в нашей стране, если вы планируете расти, то так или иначе станете работать с такими организациями. А значит, лучше знать требования этого документа и быть готовыми. Всего же под действие нового указа попадет более 500 тысяч организаций.

Что же рекомендуется делать организациям, в соответствии с данным указом?

– Установить личную ответственность за обеспечение ИБ на руководителя организации, при этом выделить отдельного заместителя генерального директора, у которого будут полномочия и ресурсы обеспечивать ИБ. При этом необходимо либо создать структурное подразделение, ответственное за обеспечение ИБ, либо возложить такие функции на существующее подразделение.

– Необходимо провести инвентаризацию договоров с подрядными организациями, оказывающими услуги по ИБ. Теперь оказывать такие услуги могут только компании, которые имеют лицензию на осуществление деятельности по технической защите конфиденциальной информации от ФСТЭК России.

– Также ещё 30 марта 2022 года были введены ограничения на приобретение иностранного оборудования и программного обеспечения для субъектов критической информационной инфраструктуры (КИИ), которые осуществляют закупки по 223-ФЗ. С 1 января 2025 г. организациям запрещается использовать средства защиты информации, произведённые в недружественных государствах, либо организациями под их юрисдикцией, прямо или косвенно подконтрольными им либо аффилированными с ними. На весну 2023 года таких стран насчитывается 48. И даже если компания-поставщик ИБ-оборудования, например, из Китая, то все равно надо проверять ее аффилированных лиц.

Забегая вперед, выскажу одно предположение. С учетом всех утечек и важности этой темы для государства можно ожидать введения некой страховки, по примеру ОСАГО. Каждую организацию могут принудить страховаться от ИБ-рисков. И тогда то, как организация будет выстраивать функцию ИБ, будет влиять на размер ее страховой премии.

Глава 3. Про общие тренды

Главный тренд в области ИБ – в отрасль приходят профессиональные менеджеры. Те, кто раньше занимались «техникой», но теперь доросли до управленцев. Они думают как о технической стороне вопроса, так и о деньгах, процессах в организации, об ответственности, которую принимают на себя. И это серьезный вызов для ИБ-компаний. Ведь им нужно уже общаться не просто со специалистами, которые в теме, а находить общий язык с менеджерами. То есть объяснять в первую очередь на языке денег и гарантий.

Второй тренд – переход от размазанной защиты по всей организации, продвижения по уровням зрелости и использования лучших практик к модели гарантированной защиты от недопустимых сценариев: нарушение технологических циклов, хищение денег, конфиденциальной информации, шифрование всех данных. То есть переход от ИБ 1.0 к ИБ 2.0.

Это связано с тем, что все уже осознают невозможность защиты от всего. Во-первых, рост цифровизации и автоматизации приводит к увеличению числа используемого ПО. А значит, экспоненциально растет и количество направлений для атак. Во-вторых, как мы уже говорили ранее, все разработчики ИТ-решений стараются снизить затраты. Например, даже мировой ИТ-гигант IBM переносит свои производства в Индию, ведь там дешевле рабочая сила программистов. При этом качество кода от большинства индийских разработчиков оставляет желать лучшего. Это как китайские реплики оригинальных товаров. Все это приводит к падению качества ПО и росту количества и критичности уязвимостей.

Плюс даже опубликованные «дыры» разработчики не спешат устранять оперативно. Тут показательна статистика от PT. Из всех выявленных и отправленных разработчикам в 2021 году уязвимостей в промышленных ИТ-системах было исправлено меньше половины – 47%. При этом известно о них становится всему миру довольно быстро – в течение нескольких часов.

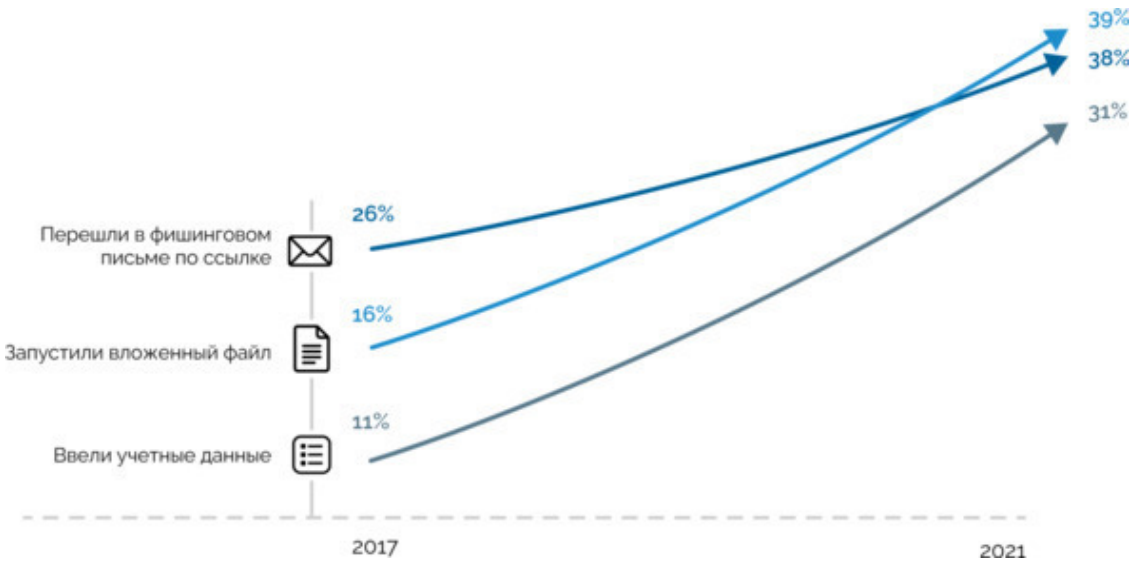
Всего же за 2022 год было выявлено и подтверждено около 25 тысяч новых уязвимостей, обнаруженных исследователями безопасности. Рост числа стартапов и выпускаемых ими программ, а также несоблюдение принципов безопасной разработки могут привести к тому, что в это число будет только увеличиваться.

В итоге и получается, что более чем в половине атак хакеры спокойно используют эти уязвимости и получают необходимый доступ за несколько минут. Сами же специалисты PT, используя известные уязвимости, смогли получить доступ к внутренней сети компаний в 60% своих проектов. А теперь добавим еще тот факт, что белых хакеров и исследователей не так уж и много, а разработчики просто не знают о всех дырах. Хакеры же не стремятся публиковать найденные уязвимости в открытом доступе. В то же время сам теневой рынок хакеров находится на подъеме.

Динамика теневого рынка

В-третьих, атаки вместо массовых становятся целенаправленными, то есть таргетированными. Как уже говорилось, если раньше таких было 43%, то сейчас на уровне 70%.

В-четвертых, как бы ни развивались технологии, узкое место – все равно люди. Так, с 2017 года количество людей, попадающихся на фишинговые письма, не только не уменьшилось, но, наоборот, кратно увеличилось. И в топе наиболее используемых и эффективных способов проникновения в компанию по-прежнему остается фишинг с помощью электронной почты. При этом темы рассылок, которые люди открывают чаще всего, остаются неизменными из года в год: зарплата, премии, социальные программы, ДМС, резюме. Кроме того, лучше всего работают рассылки, посвященные событиям в конкретной компании или подразделении. То есть растет роль социальной инженерии.



При этом интересна статистика атак на обычных людей. Ведь бесконечные утечки персональных данных упрощают работу хакеров с точки зрения выбора нужных людей при планировании атаки на организацию. Так, в 2021 году в 58% атак хакеры заражали устройства пользователей вредоносным ПО: это были приложения для удаленного управления (34%), шпионское ПО (32%) и банковские трояны (32%). При этом к концу 2022 года шпионское ПО использовалось уже в 49% успешных атак.

По итогам 2022 года чаще всего источником заражения становились фишинговые сайты (42% успешных атак) и письма электронной почты (20%). Также хакеры объединяли личные устройства людей и организовывали так называемые ddos-атаки, то есть просто перегружали ИТ-инфраструктуру организации-жертвы. И в массовых фишинговых атаках хакеры использовали актуальную новостную повестку: покупка поддельных сертификатов о вакцинации, создание мошеннических сайтов перед чемпионатом Европы по футболу, премьерой нового эпизода сериала «Друзья» или другого «вкусного» события.

Ну, и в-пятых, менеджеры – люди прагматичные, они хотят гарантий. В итоге мы и пришли ко второму тренду – формулированию простых и понятных для топ-менеджеров запросов, чтобы недопустимое невозможно было реализовать.

По моему мнению, это вполне нормальная ситуация. Бесконечно наращивать броню и закрываться невозможно. Если вы любите погонять в танки, то помните пример с танком Маус, который в итоге стал неповоротливым и в жизни вообще не мог передвигаться, став лишь музейным экспонатом. При этом развитие техники все равно сделало его пробиваемым. В борьбе брони и снаряда всегда в итоге выигрывает снаряд.

Возвращаясь к языку бизнеса, поделюсь наблюдением. Наращивание брони порой приводит к росту бесполезной бюрократии. Я видел компании, которые закрывались так, что останавливались бизнес-процессы, и люди просто выходили за контур компании, начинали вести рабочую коммуникацию и обмен документами в открытых мессенджерах и личной почте. Ведь у них есть KPI и с них требуют результат. А ждать по неделе-две пока техподдержка решит очередную проблему, они не могут. В итоге хотим защититься, но только множим риски.

Третий тренд – развитие киберполигонов и кибербитв, которые предоставляют возможность специалистам по кибербезу пробовать свои силы в обнаружении и пресечении действий злоумышленников, тестировать инфраструктуру и получать информацию для анализа и развития. Также с начала 2023 года идет активное создание программ по поиску уязвимостей за вознаграждение. Такие программы называются Bug bounty. Это позволяет «белым» хакерам и исследователям применять свои знания во благо и получать за это вознаграждение. В основ-

ном это относится к финансовой сфере (программы поиска уязвимостей) и крупным корпорациям (участие в кибербитвах).

Глава 4. Что происходит в отраслях

Атаки на корпорации и организации становятся все больше похожими на спланированные военные операции – идут атаки и на оборудование, и на людей. Так, мы уже с вами знаем про фишинг, использование уязвимостей и так далее. Но, помимо этого, существуют и специализированные компании, которые занимаются разработкой инструментария для проникновения в различные информационные системы. Особенно это развито в тех странах, где такая работа не попадает под ограничения законодательства. То есть в принципе это не нелегальный бизнес, и с учетом текущей ситуации многие страны, скорее всего, вообще начнут закрывать глаза на него.

Государственное управление и организации

Государственные организации сейчас, в 2022—2023 годах, проходят настоящее боевое крещение. В 2022 году число успешных атак на государственные учреждения увеличивалось в каждом квартале. Госучреждения столкнулись с наибольшим числом инцидентов среди любых организаций. На их долю пришлось 17% от общего числа успешных атак (в 2021 году этот показатель был 15%). Всего за 2022 год PT зафиксировали 403 инцидента с государственными организациями, что на 25% больше, чем в 2021 году.

Основной способ атаки – социальная инженерия. Цель атак – данные. И это понятно, ведь автоматизация и цифровизация в гос. управлении идет полным ходом. А значит, государственные органы начинают генерировать большие данные: налоги, медицинская информация, биометрия и т. д. Медицинские данные представляют для хакеров особый интерес, в том числе и для целей социальной инженерии, повышения эффективности фишинговых атак.

Наиболее популярными типами вредоносного ПО оказались шифровальщики (56%) и программы для удаленного управления (29%). Также постоянно растет доля атак на вебресурсы, – в 2020 году таких было 14%, к концу 2022 – 41%.

Причем госструктуры под ударом не только у нас в стране.

Пример 1

В середине октября 2021 года хакер получил доступ к базе данных правительства Аргентины, в которой содержится информация обо всех удостоверениях личности граждан. В итоге на черном рынке были выставлены на продажу данные и ID-карты всего населения Аргентины, то есть более 45 млн граждан. Причем в качестве подтверждения достоверности данных хакер раскрыл информацию о 44 известных личностях, в том числе президента страны.

Пример 2

Полицейское управление столицы США Вашингтона. Там случилась массовая утечка внутренней информации после атаки программы-вымогателя. В дарквебе (сегмент Интернета, который скрыт от обычных пользователей, где продают поддельные документы, оружие, наркотики, получают заказы хакеры) были опубликованы тысячи конфиденциальных документов. Также были обнаружены сотни личных дел полицейских, данные об информаторах и разведывательные отчеты со сведениями, полученными от других государственных органов, включая ФБР и Секретную службу.

Пример 3

Атакой шифровальщиком данных хакеры вызвали коллапс IT-инфраструктуры трех больниц в США, сорвали несколько плановых операций, нарушили процесс приема пациентов и похитили 1,5 ТБ персональных данных, включая медкарты. Группировка получила выкуп в размере 1,8 млн долларов за дешифратор и непубликацию похищенной информации. А кибератака вымогателей на одну из главных больниц Барселоны (Clinic de Barcelona) привела

к повреждению ИТ-инфраструктуры клиники и вынудила отменить 150 неотложных операций и до 3000 обследований пациентов (по данным Associated Press).

Пример 4

Также интересный случай был в ноябре 2022 года. На одном из форумов в дарквебе появилось сообщение о взломе инфраструктуры Федеральной налоговой службы России. Хакеры утверждали, что скачали 800 Гб конфиденциальной информации. Официальных комментариев ведомства не поступило. В качестве доказательств прилагались ссылки на несколько проектов, которые, по сообщению хакеров, взяты из базы данных ФНС. «На то, чтобы проникнуть в сеть налоговой, нам понадобилось всего одну неделю времени, а во взломе участвовали лишь три человека. На самом деле, нами уже захвачено несколько десятков государственных структур такого уровня. Но заявлять о них надобности пока нету», – написали хакеры в сообщении.

При этом еще один курьезный случай с ФНС произошел в 2019 году. Тогда была возможность получить доступ к двум базам данных. Первая содержала более 14 млн данных о людях, а вторая – 6 млн. В них можно было найти имена, адреса, номера паспортов, данные о месте проживания, номера телефонов, номера ИНН, названия компаний-работодателей, а также информацию об уплаченных налогах.

Пример 5

Атака вымогателей на госучреждения Коста-Рики в апреле 2022 года. Группировка вымогателей Conti напала на госучреждения Коста-Рики и потребовала выкуп в размере **20 млн долларов**. Из-за недоступности большей части IT-инфраструктуры в стране было объявлено чрезвычайное положение, а несколько позже к атакованному государственному сектору присоединилось здравоохранение Коста-Рики, учреждения которого атаковала группировка Hive.

Пример 6

Власти города Берлингтон в Канаде подверглись фишинговой атаке, в результате которой 503 000 долларов США были переведены не настоящему поставщику услуг, а киберпреступнику.

Промышленность и энергетика

Промышленность все больше привлекает киберпреступников: количество атак в 2021 году превосходит результаты 2017 года более чем в 7 раз. А в 2022 году около 10% всех успешных атак пришлось на промышленность. При этом промышленные компании, по сути, не готовы противостоять сложным атакам и вредоносному ПО. Так, 95% компаний либо не защищают свои автоматизированные системы управления технологическими процессами (АСУ ТП) специальными решениями, либо делают это частично. И системного подхода к управлению кибербезопасностью, например, управления уязвимостями и обновлениями компонентов ПО, в 93% случаев тоже нет. Это с учетом того, что ущерб от остановки бизнес-процессов может быть катастрофичным, в том числе с повреждением и разрушением оборудования, техногенными катастрофами. Компаниям проще идти на поводу у хакеров и тихо выплачивать выкуп.

Спасает сейчас то, что злоумышленникам просто невыгодно заниматься изучением технологических параметров, разбираться, что именно надо изменить, ведь можно просто зашифровать или украсть конфиденциальные данные. По моему мнению, это ключевой сдерживающий фактор.

Также здесь сохраняется и общий тренд – атаки становятся все более комплексными:

– использование вредоносного ПО (71% успешных атак)

– социальную инженерию (около 50%)

– эксплуатацию уязвимостей в ПО (41%).

Само вредоносное ПО распространялось через ИТ-оборудование (49% случаев) и почту (43%). Перебои в работе из-за вмешательства в технологические и бизнес-процессы возникали в 47% случаев. И главным образом из-за шифровальщиков данных и ПО для удаления данных (вейперов). В течение 2022 года доля шифровальщиков увеличивалась с 53% в первом квартале до 80% в третьем. Доля вейперов достигла 7% (в 2021 году их было 1—2%).

Рост доли эксплуатации уязвимостей в атаках говорит о том, что эти методы экономически целесообразны, а это уже свидетельствует о низком уровне защиты в промышленности. И именно в программных и аппаратных продуктах, предназначенных для промышленности, в 2021 были обнаружены и исправлены наиболее опасные уязвимости.

Промышленники и энергетики вроде и осознают все риски, но и специфика отрасли не дает возможности проводить полномасштабные учения с отработкой практических сценариев и выявлением недопустимых событий. Поэтому сейчас появляются киберполигоны, где можно через виртуальную или дополненную среду без риска сломать процессы и оборудование, проводить любые учения и оценивать последствия. Один из таких примеров – мероприятие Standoff, которое организовывают PT.

В целом, в 2021 году интересы хакеров в России по отраслям промышленности распределились следующим образом:

– 31% авиакосмическая отрасль;

– 23% государственные организации;

– 23% IT-компании;

– 15% военно-промышленный комплекс;

– 8% топливно-энергетический комплекс.

Что касается статистики PT, то в своих проектах с первой половины 2020 по вторую половину 2021 года им удалось реализовать 87% недопустимых событий.

Финансы

Финансовый сектор – один из тех, кто чувствует себя относительно хорошо. Доля атак на эти организации от общего числа снижается из года в год. И что интереснее всего, новых группировок, стремящихся выводить деньги со счетов в банках, не появляется. Причина этому – зрелость отрасли и усилия Центробанка: регламенты, вложения в ИТ-инфраструктуру и ПО, налаженный информационный обмен. И это понятно, если воруют деньги, то это видно здесь и сейчас.

Атакуются организации вновь через социальную инженерию (47%) и использование вредоносного ПО (загрузчики, шпионское ПО, трояны, шифровальщики.

Типичными целями атак на банки стали хищение конфиденциальной информации и остановка ключевых бизнес-процессов (53% и 41% случаев соответственно). Хищение денег было в 6% успешных атак.

Сейчас финансовые организации атакуются с целью:

– получения более выгодного курса обмена валют;

– кражи денег со счетов пользователей или обмана комиссии;

– получения конфиденциальной информации о пользователе и её использования в других атаках при помощи социальной инженерии;

– увеличения нагрузки на систему и сбоев в работе личных кабинетов пользователей.

Кроме того, все еще встречаются небезопасные реализации систем быстрых платежей.

В результате банки внедряют все новые технологии защиты:

– ужесточают проверки KYC (обязательная проверка персональных данных клиента), в том числе развиваются сервисы проверки документов (видеозвонки с распознаванием доку-

ментов, загрузка фотографий документов, проверки по базам данных, оценка социальной активности) для понимания, реальный ли человек скрывается за тем или иным аккаунтом;

– вводят системы машинного обучения для ускорения, упрощения и улучшения поиска информации о клиенте, распознавания и блокирования подозрительных операций.

В итоге количество стандартных веб-уязвимостей уменьшается, но количество логических уязвимостей, наоборот, увеличивается. И во многом это происходит из-за развития экосистем: создание все новых и более сложных интеграций, микросервисов, введение голосовых помощников и чат-ботов.

Однако, есть два негативных фактора, позволяющие специалистам PT находить в каждой организации уязвимости, которые дают возможность проникнуть во внутреннюю ИТ-инфраструктуру. Во-первых, защитные патчи, которые выпускают разработчики ПО, зачастую игнорируются ИТ-службами организаций и не устанавливаются. Во-вторых, всегда есть вероятность наличия уязвимости, о которой пока неизвестно разработчикам, но ее обнаружили исследователи злоумышленников. Такие уязвимости называют «уязвимостями нулевого дня». И эти факторы – залог того, что хакер проникнет внутрь инфраструктуры, поэтому нужно учиться их вовремя выявлять.

Всего в ходе исследований специалисты PT смогли проникнуть во внутреннюю сеть организаций в 86% случаев. Также исследователи PT получали полный контроль над инфраструктурой и реализовывали недопустимые события: доступ к критически важным для банков системам, к АРМ казначеев, серверам обмена платежными поручениями. Всего экспертам PT удалось реализовать более 70% недопустимых событий в каждой финансовой организации.

В итоге вымогатели продолжат свои атаки на банки. Пока эти атаки проще в исполнении и в совокупности приносят больше прибыли, чем попытки вывести крупную сумму денег со счетов. Но теперь одной из основных целей хакеров будут клиенты банков, которые пользуются онлайн-банкингом. По данным Центробанка России уже в 2020 году 75% взрослого населения пользовались онлайн-банкингом. Поэтому хакеры продолжат развивать направление компрометации банковских приложений. Также в ходу останутся приемы социальной инженерии.

Основным же методом также является фишинг – на него приходится 60% атак. Хакеры с удовольствием получали кредиты на чужие имена, чужие фирмы, которым эти кредиты теперь нужно выплачивать.

В результате, если раньше рентабельно было атаковать компании с целью кражи денег со счетов, то работа, которую провел регулятор, и развитие систем защиты снижают привлекательность финансовых компаний, нужна слишком высокая компетентность и техническое оснащение. Но вот с промышленностью всю наоборот. Там хакерам как раз интересны данные о клиентах, внутренних пользователях и любая информация, которая относится к коммерческой тайне.

Опять же, это приводит и к росту атак на конфиденциальные данные (с 12% до 20%). Также популярны персональные данные (32%), учетные данные (20%) и медицинская информация (9%).

На обычных людей в целом было направлено 14% атак, и в 88% случаев через социальную инженерию. И конечная цель в 66% случаях – учетные и персональные данные.

Закрывая главу, приведу еще несколько примеров наиболее резонансных атак 2022 года на организации из коммерческого сектора:

– Группировка Lapsus$ взломала ряд крупных IT-компаний. Сначала была атакована Okta, которая разрабатывает решения для управления учетными записями и доступом, в том числе обеспечивает поддержку многофакторной аутентификации. Затем атаковали разработчика графических процессоров Nvidia, в результате чего был украден 1 ТБ данных, среди которых – исходный код драйверов видеокарт и сертификаты для подписи ПО. Украденные

сертификаты Nvidia использовались для распространения вредоносных программ. В марте преступники смогли взломать Microsoft и Samsung, украв исходный код некоторых продуктов.

– Швейцарская компания Swissport, являющаяся провайдером грузовых авиаперевозок и работающая в 310 аэропортах в 50 странах мира, подверглась атаке программы-вымогателя. Атака привела к задержкам множества рейсов и утечке 1,6 ТБ данных.

– Атака на телекоммуникационного оператора Vodafone в Португалии вызвала сбои в обслуживании по всей стране, в том числе в работе сетей 4G и 5G. Vodafone Portugal обслуживает более 4 млн абонентов сотовой связи.

– В октябре в результате кибератаки на Supeo, поставщика IT-услуг для крупнейшей датской железнодорожной компании, на несколько часов остановилось движение поездов. Supeo предоставляет решение, которое машинисты используют для доступа к критически важной информации – данным о работах на путях и об ограничениях скорости. Во время атаки поставщик отключил свои серверы, что вызвало сбои в работе приложения, и машинисты были вынуждены останавливать составы. После восстановления движения поезда еще сутки не ходили по расписанию.

– В марте Toyota на день приостановила работу 14 заводов в Японии из-за кибератаки на Kojima Industries, поставщика комплектующих. Кибератака также затронула других японских производителей автомобилей – компании Hino и Daihatsu Motors.

– Во II квартале произошла крупная атака на 3 иранских сталелитейных завода, в результате которой были нарушены технологические процессы, а на одном из заводов злоумышленникам удалось обрушить ковш с жидким чугуном и вызвать пожар.

Глава 5. Про технологии

Облачные технологии

Одной из самых востребованных технологий цифровизации и цифровой трансформации являются облачные вычисления, хранилища и сервисы. Соответственно, фокус в организации ИБ все больше смещается в область ответственности провайдеров. Тут необходимо смотреть с двух углов:

– крупные провайдеры облачных сервисов и инфраструктуры;

– локальные стартапы и небольшие провайдеры.

Что касается первых, то здесь все неплохо: крупные провайдеры осознают, что их будут атаковать, а значит, будут предпринимать меры. Предупреждён – значит вооружён. И в целом облачные сервисы крупных провайдеров разрабатываются по принципу «вокруг все враги», плюс они имеют компетентных специалистов по ИБ. Также подобная централизация позволяет меньшим количеством специалистов защитить большее количество данных.

А вот относительно стартапов и небольших провайдеров все печальнее. У них нет ресурсов, и скорее всего они потеряют большую часть самых денежных клиентов. То же самое относится к локальным ЦОДам и службам ИТ, которые развиваются внутри промышленных компаний. Они, как правило, не способны обеспечить необходимый уровень защиты. Либо, как говорили ранее, начинают просто уходить в глухую оборону, и для бизнеса теряется всякий смысл таких облачных сервисов, ими просто невозможно пользоваться. В то же время растет и количество вредоносного ПО для Linux.

Заставляет задуматься и тот факт, что почти 40% всех выявленных и закрытых в 2021 году уязвимостей с помощью исследователей от PT имели высокий уровень опасности. А самое важное, что 12,5% всех уязвимостей были выявлены в софте, призванном обеспечивать защиту от хакерских атак. И, несмотря на всю текущую ситуацию и санкции, ребята из PT соблюдают responsible disclosure – политику в отношении найденных уязвимостей, т.е. сообщают разработчикам о всех найденных уязвимостях до их публикации в открытом доступе.

Мобильные приложения

Второе направление, которое развивается вместе с цифровизацией, – мобильные приложения: для клиентов и программы лояльности, для сотрудников, мобильные обходчики, фиксация опасный событий, государственные услуги. Любая более-менее крупная организация имеет свое приложение.

При этом, по данным PT, самая популярная уязвимость мобильных приложений – хранение пользовательских данных в открытом (или легко обратимом) виде. Также встречалась ситуация, когда важные данные хранились в общедоступных каталогах. А общая доля недостатков, связанных с небезопасным хранением данных, составила более 33% от всех найденных уязвимостей. То есть то, что интересно хакерам, и является одной из самых частых проблем.

Эксперты PT в 2022 году провели исследование 25 пар приложений (Android – IOS). Практически каждое имело проблемы с хранением данных. Одна из ключевых причин – чрезмерная вера разработчиков в системные механизмы защиты на уровне операционной системы, игнорирование многоуровневой защиты.

Наибольшая доля уязвимостей (14%) пришлась на хранение пользовательских данных в открытом виде. Второе место поделили между собой уязвимости, касающиеся проверки целостности приложений и хранения конфиденциальной информации в коде (по 9%).

Также, практически каждое приложение имеет хотя бы один из следующих недочетов:

– отсутствие обнаружения взлома операционной системы (root на Андроиде и jailbreak на IOS);

– отсутствие контроля целостности исполняемых файлов;

– отсутствие обфускации (запутывания кода).

Android и iOS: кто безопаснее?

Android-приложения всегда считались лакомой целью для хакеров: открытая система, широкие возможности, легко оставить дыру в приложении. С IOS всегда было наоборот: у разработчиков мало возможностей сделать ошибку и оставить открытыми ненужные «двери». И была некая парадигма – покупаем для ТОПов устройства на iOS, и они защищены. Но сейчас идет изменение этого тренда. Google все больше ограничивает возможности приложений, заставляет разработчиков указывать необходимую функциональность. А согласно недавним новостям, в Android 14 полностью заблокируют возможность установки устаревших приложений. Причем как через магазин приложений, так и через самостоятельное скачивание установочных файлов. В iOS, наоборот, приложениям становятся доступны новые способы взаимодействия с операционной системой и друг с другом. В общем, граница между платформами стирается, и использовать iOS устройства для ТОПов в надежде на абсолютную безопасность становится слишком рискованным занятием.

Конец ознакомительного фрагмента.