

Оценка киберзащищенности российского бизнеса

2019 год



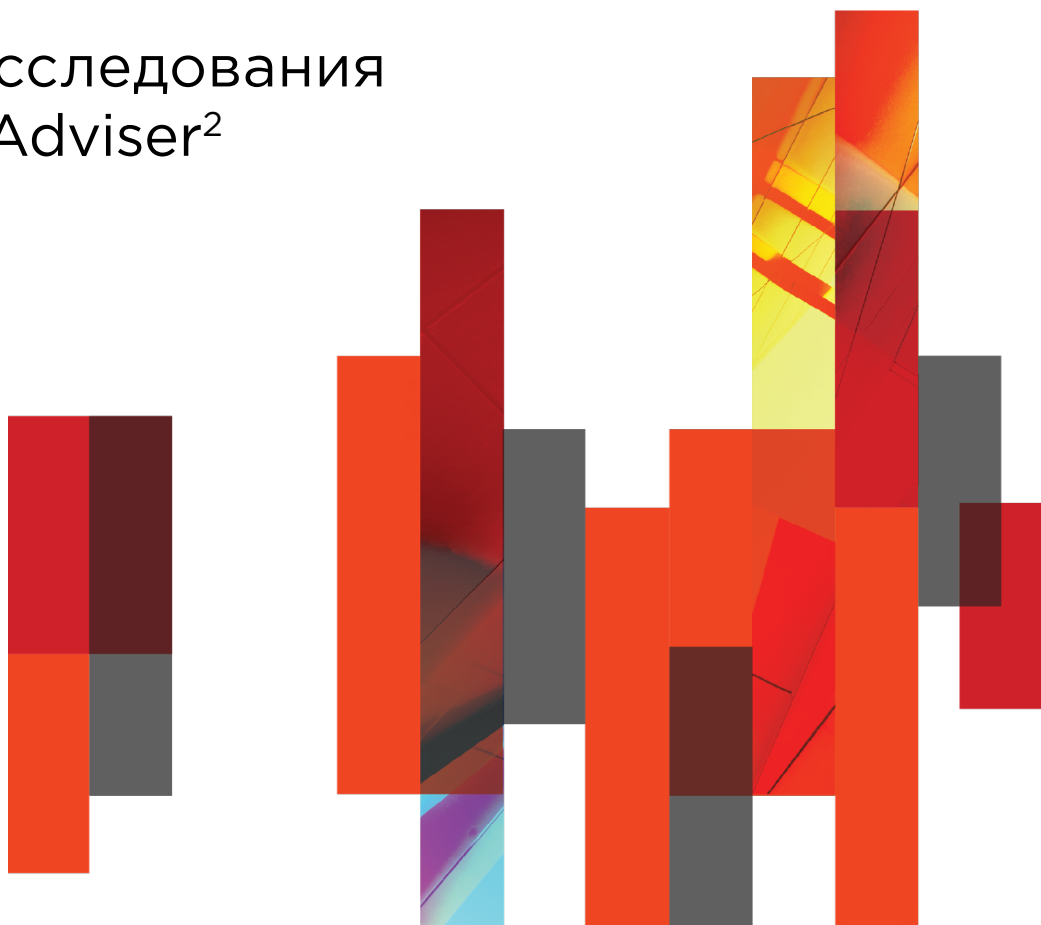
г. Москва, 2019 г.

Содержание

Кибербезопасность в российских компаниях	2
Результаты исследования Microsoft и TAdviser	
Цели и задачи исследования	3
Методика	3
Выборка	3
Уровень осведомленности	4
Практический опыт	4
Финансовые показатели	6
Оценка рисков	6
Выводы	7
АРТ-атаки глазами сотрудников российских компаний	8
Результаты исследования Positive Technologies	
Об исследовании	9
Цели и последствия атаки	10
Линия обороны	12
Кадры играют важную роль	14
Сможет ли компания противостоять АРТ	15
Как защититься?	17
Рекомендации от Microsoft и Positive Technologies	
Как защититься, если вы обычный пользователь?	18
Как защититься, если вы организация?	19

Кибербезопасность в российских компаниях

Результаты исследования
Microsoft¹ и TAdviser²



1. Microsoft (Nasdaq «MSFT» @microsoft) обеспечивает условия для цифровой трансформации в эпоху «интеллектуального облака» и «интеллектуальных технологий». Миссия компании — дать возможность каждому человеку и организации на планете достичь большего.
2. Аналитики TAdviser с 2005 года провели десятки исследований в интересах заказчиков и поставщиков IT-систем. В течение многих лет TAdviser формирует уникальную базу проектов российских компаний из 37 отраслей экономики по внедрению информационных систем различных поставщиков. Среди клиентов: ГИВЦ Москвы, ФСК ЕЭС, «Энергодата», Baltshug Kempinski, «Спортмастер», Stockmann, «Самохвал», «Бахетле», «Русский Стандарт Страхование», SAP, Microsoft, Oracle, «Ситроникс», IBS, R-Style, Abbyy, SAS Institute, «РДТех», QlikTech, «Галактика», «Техносерв», «БДО Юникон», «Энвижн Груп», «АйТи» и многие другие организации.

Цели и задачи исследования

В ходе настоящего исследования планировалось определить уровень осведомленности российского малого и среднего бизнеса (представляющего различные отрасли экономики) об угрозах кибезопасности и статистике инцидентов, а также дать оценку динамике киберпреступлений за последний год, включая наиболее популярные цели и каналы атак.

Методика

Формат работ — полевое исследование. Для выполнения задач исследования был проведен телефонный опрос экспертов, представляющих 450 российских компаний.

Для проведения опроса была сформирована база респондентов — руководителей IT-подразделений, руководителей направления ИБ, руководителей функциональных подразделений, а также других лиц, влияющих на принятие решений в области ИТ и ИБ.

Выборка

Опрос проводился в сегменте малого и среднего бизнеса.

Респонденты представляли следующие отрасли экономики: финансы и страхование, ритейл, e-commerce, FMCG, промышленное производство, транспорт, энергетика и ЖКХ и др.

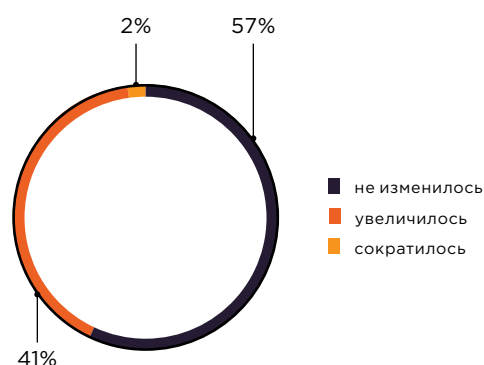
В опросе участвовали руководители ИТ (CIO), руководители служб ИБ и их заместители и другие представители компаний, влияющие на вопросы обеспечения ИБ.



Уровень осведомленности

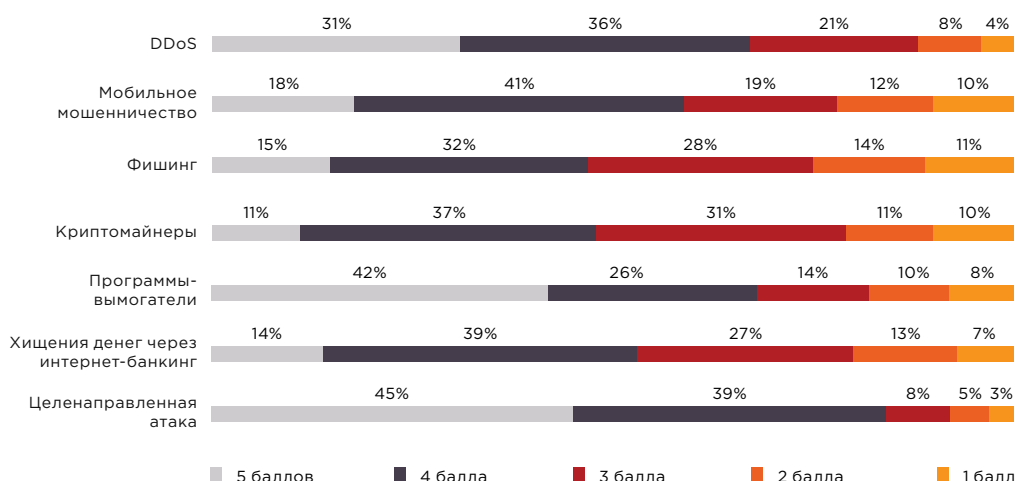
По данным проведенного опроса, 76% предприятий СМБ из разных отраслей экономики сталкивались за последний год с инцидентами информационной безопасности (ИБ). Многие респонденты отмечают усиление масштаба киберпреступлений за последнее время. Около трети участников опроса, не сталкивавшихся с инцидентами ИБ за последнее время, допускают, что могли их просто не обнаружить. В целом рост киберпреступности опрошенные компании связывают с ежегодно повышающимся уровнем цифровизации бизнеса и общества.

Оценка динамики инцидентов ИБ в 2018 — 2019



В перечне наиболее опасных угроз большинство респондентов выделяют целенаправленные атаки (45% оценили эту угрозу в максимальные 5 баллов), программы-вымогатели (42% оценили в 5 баллов) и атаки DDoS (31% присвоили 5 баллов). Именно с такого рода инцидентами большинство опрошиваемых сталкивалось в 2018 г.

Оценка наиболее опасных угроз

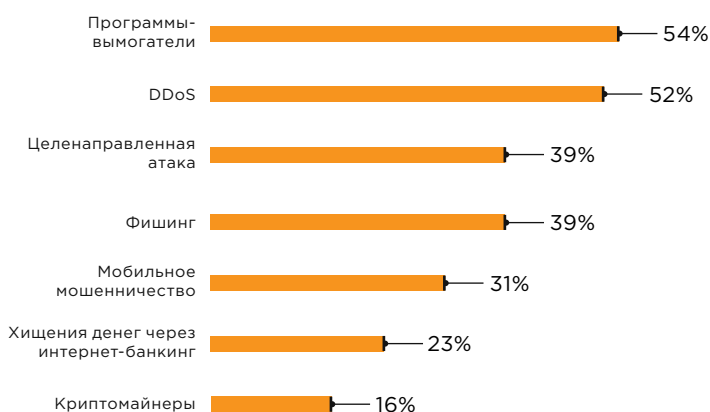


Практический опыт

Большинство опрошенных (76%) подтвердили, что фиксировали хотя бы один инцидент информационной безопасности за последний год. Чаще всего респонденты сталкивались с программами-вымогателями (54%), DDoS (52%), целенаправленными атаками и фишингом (по

39%). Рост DDoS-атак объясняется их относительной дешевизной при высокой эффективности, при этом возрастает мощность атак, отмечают в первую очередь представители сегмента e-commerce (интернет-магазины и различные интернет-сервисы). Наибольшую закрытость в вопросах данной тематики проявляли традиционно организации финансового сектора.

Выявление инцидентов ИБ в 2018 — 2019



Среди других зафиксированных инцидентов респонденты наиболее часто указывают утечки информации по вине инсайдеров (14%) — ввиду как умышленных мошенничеств, так и по причине низкого уровня киберграмотности сотрудников.

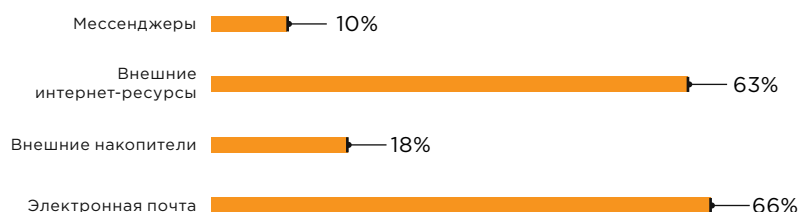
Большинство респондентов, столкнувшихся с киберпреступлениями за последний год, отмечают, что их целью были денежные средства либо номера банковских карт, счетов (37%). Около 15% компаний, подтвердивших факт инцидента ИБ, прокомментировали, что не понесли ущерба, адекватно отразив атаку. Нужно отметить, что часто отсутствием ущерба считается возможность решить проблему собственными силами — за счет персонала компании.

Наиболее частые цели кибератак



К основным каналам угроз респонденты относят в первую очередь электронную почту (66%) и внешние интернет-ресурсы (63%).

Основные каналы киберугроз



Финансовые показатели

Более трети опрошенных затрудняются с оценкой возможного размера ущерба от атаки — точные цифры, как показал опрос, не может привести практически никто. Ориентируясь в предложенных диапазонах, 57% отметили, что понесли незначительный ущерб — до 100 тыс. руб. Здесь нужно учитывать, что респонденты представляют сегмент СМБ. Крупные компании, в свою очередь, по данным TAdviser, также редко раскрывают реальный размер ущерба и апеллируют к отсутствию адекватной оценки и методики ее получения.

Участники опроса часто затрудняются с ответом на вопрос о затратах на ликвидацию последствий кибератак. Как правило, размер затрат близок к той сумме, в которую оценивается (условно) сам ущерб. Речь здесь идет преимущественно о закупке необходимого ПО, проведении мер по комплексному усилению защиты (больше применимо к респондентам, представляющим средний бизнес, и не всегда применимо в силу ограниченности бюджета ИТ или ИБ к малым предприятиям).

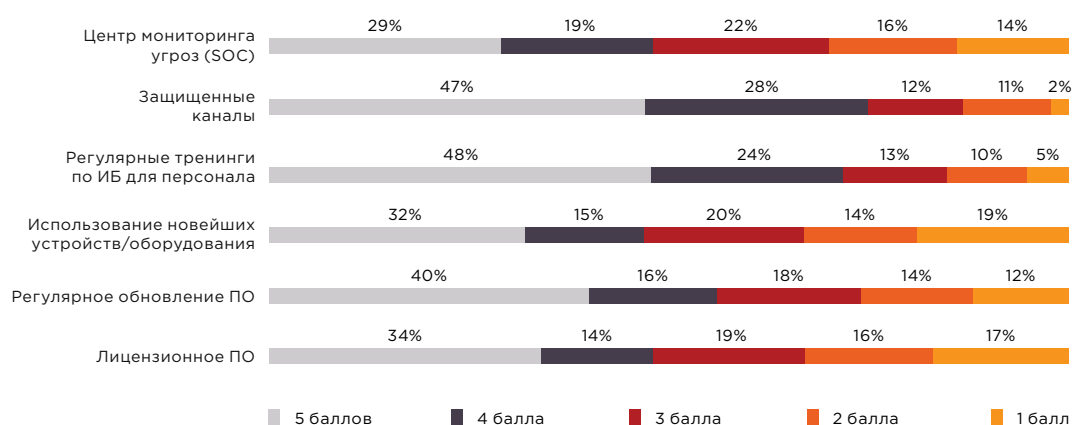
На восстановление от последствий атак у более трети опрошенных уходило несколько часов. Еще более трети затратили сутки и более на ликвидацию негативных эффектов от инцидентов.

Оценка рисков

Подавляющее большинство респондентов отмечают увеличение количества инцидентов ИБ за последний год. Представители опрошенных компаний говорят в том числе и о появлении новых видов угроз (например, связанных с мобильными приложениями и устройствами). Аналогично отмечается и рост ущерба от кибератак.

К наиболее эффективным мерам защиты от киберпреступлений около половины респондентов относят регулярные тренинги по ИБ для персонала и использование защищенных каналов (эти пункты оценили на 5 баллов 48% и 47% соответственно). Еще 40% подчеркивают значимость регулярного обновления программного обеспечения и более трети — использование новейших устройств и оборудования в организации.

Оценка эффективности мер защиты от инцидентов ИБ



Свою готовность обеспечить работу географически распределенных команд подтвердили 39% опрошенных, в том числе 24% — работу с использованием мобильных устройств (вне периметра корпоративной сети). Это подразумевает достижение определенного уровня зрелости в подходах к обеспечению безопасности работы в облачной среде, когда сотрудники получают доступ к критической информации в режиме реального времени из любой точки и с разных устройств.

Выводы

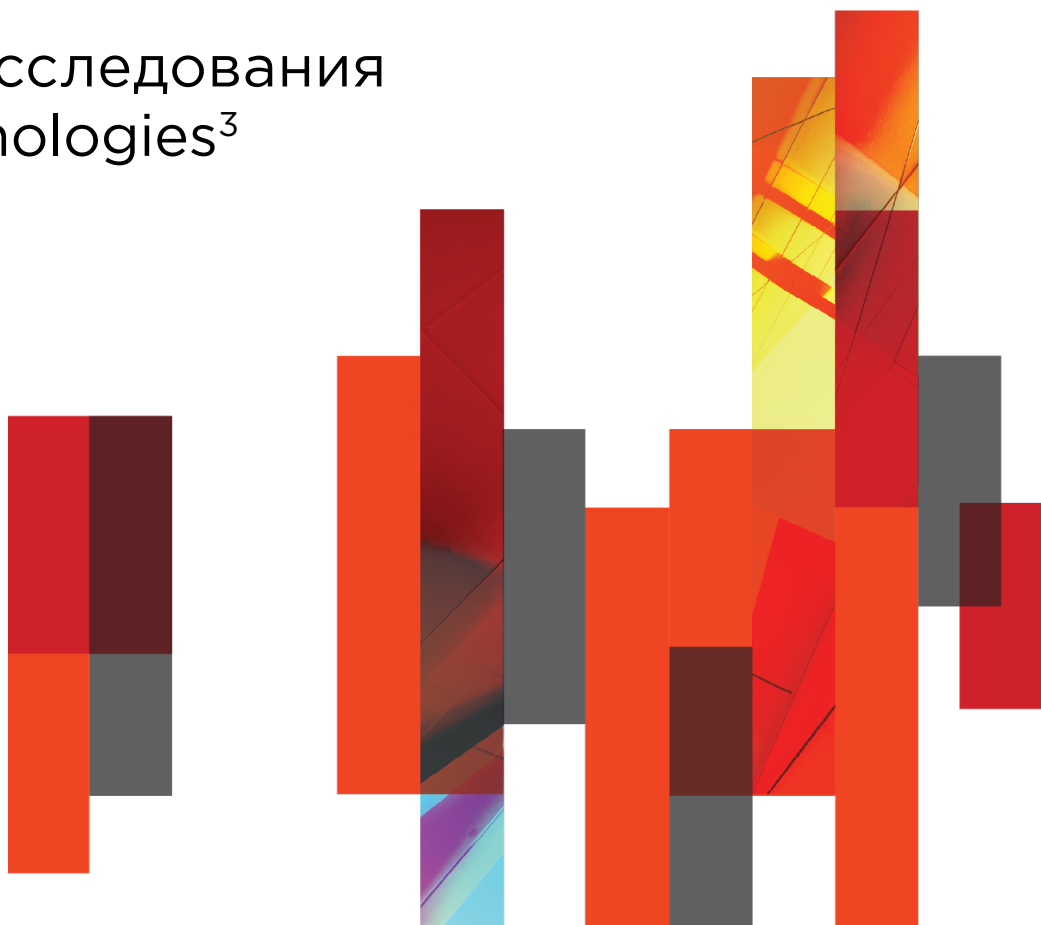
Как показало проведенное исследование, большинство компаний СМБ из разных отраслей сталкивались за последний год с киберпреступлениями. К основным каналам угроз респонденты относят электронную почту и внешние интернет-ресурсы. Наиболее опасными угрозами большинство считают целенаправленные атаки, программы-вымогатели и атаки DDoS.

Исследование выявило, что в компаниях до сих пор не сформировался подход к оценке ущерба от кибератак в финансовых показателях. Большинство респондентов затрудняются с обозначением суммы ущерба, не располагая точными данными.

В числе наиболее эффективных мер противодействия киберугрозам около половины опрошенных указывают повышение киберграмотности — за счет регулярного обучения персонала в области ИБ, а также использование защищенных каналов и регулярное обновление программного обеспечения.

APT-атаки глазами сотрудников российских компаний

Результаты исследования
Positive Technologies³



3. Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов. Подробнее — на ptsecurity.com, facebook.com/PositiveTechnologies, facebook.com/PHDays.

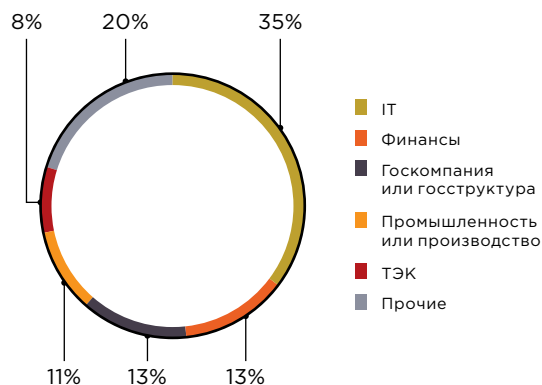
Об исследовании

Есть люди, которые не относятся серьезно к киберугрозам, кибератакам. А есть те, кто ежедневно борется за защиту своих компаний от хакеров. Речь идет о технических специалистах — сотрудниках отделов ИТ и ИБ. Именно они работают с теми системами защиты, которые внедряются в организации: настраивают, контролируют, реагируют на инциденты и восстанавливают рабочие процессы в случае необходимости. Поэтому их мнение для нас важно и именно они могут дать корректные ответы на наши вопросы. Кому как не им знать, готовы ли российские организации дать отпор киберпреступникам?

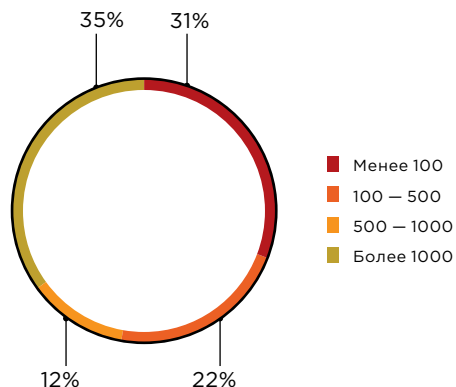
Мы продолжаем поднимать вопросы противостояния сложным целенаправленным атакам (advanced persistent threat, APT). Мы провели опрос среди посетителей сайта компании Positive Technologies, аудитории интернет-портала SecurityLab.ru⁴ и участников ряда отраслевых сообществ⁵, чтобы узнать, как они оценивают угрозу APT. Этот эксперимент пусть и предоставил небольшую выборку данных для анализа, но позволил нам посмотреть на вопросы защиты от APT глазами технических специалистов, и картину, которую мы увидели, мы и хотим показать.

В опросе приняли участие 306 респондентов, представляющих компании различных отраслей.

Распределение компаний по отраслям



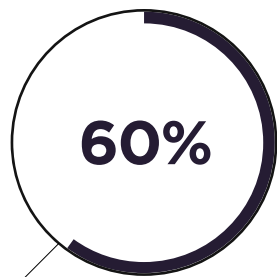
Распределение компаний по численности штата



С кем приходится бороться?

Хакеры, входящие в состав АРТ-группировок, имеют большой опыт, высокую квалификацию и хорошие технические навыки. Кроме того, они обладают таким ценным ресурсом, как время, и могут тщательно подходить к вопросу организации атак.

4. Сайт Securitylab.ru — один из лидеров российского Интернета в сфере сетевых технологий информационной безопасности. Ежемесячная аудитория портала насчитывает около полумиллиона посетителей ежемесячно, большая часть из которых — программисты, ИТ- и ИБ-специалисты, руководители соответствующих отделов.
5. Совокупная аудитория сообществ более 16 000 ИТ- и ИБ-экспертов из различных сфер отечественного бизнеса.



респондентов считают риск успешной АРТ-атаки опасным для компании

для СМБ этот показатель составляет **52%**

Цели и последствия атаки

Киберпреступления зачастую совершаются ради финансовой прибыли. Однако цели конкретной атаки зависят от сферы деятельности компании-жертвы. Например, атака на информационные системы государственных учреждений, как правило, проводится для кражи конфиденциальной информации (шпионажа). Мотивами также могут быть саботаж, подрыв репутации государственных структур, дестабилизация политической обстановки. При атаке на банк злоумышленники стремятся пополнить свои счета через несанкционированные транзакции. В промышленных компаниях и организациях топливно-промышленного комплекса хакеры могут охотиться за информацией, позволяющей добиться конкурентного преимущества на рынке: данными исследований и используемыми технологиями. Также целями атаки может быть нарушение нормальной работы предприятий.

По каким причинам компания может стать целью АРТ-группировок (доля респондентов, представляющих компании из отдельных отраслей)

Кража денег со счетов компании (или ее клиентов)

76% Финансовая отрасль

Кража конфиденциальной информации (шпионаж)

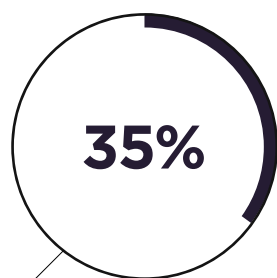
75% Государственные учреждения

Остановка бизнес-процессов и вывод из строя инфраструктуры

60% ТЭК

Нарушение технологического (производственного) процесса

59% Промышленные компании

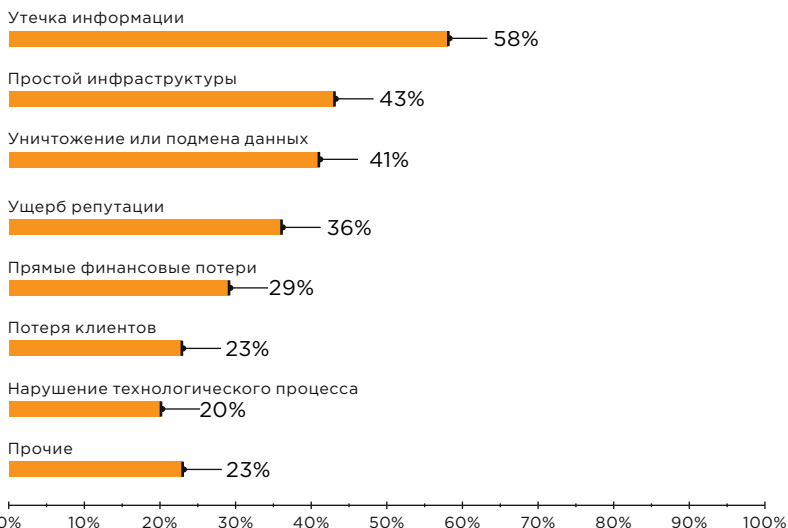


респондентов считают, что их компании не подвергались атакам либо атаки не имели успеха

для СМБ этот показатель составляет **33%**

Только 56% респондентов смогли назвать последствия атак, с которыми столкнулись их компании. Остальные или затруднялись дать ответ, или были уверены, что организация не подвергалась кибератакам (либо атака не имела успеха).

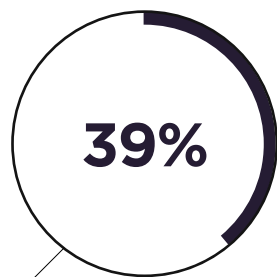
С какими последствиями кибератак сталкивались компании



Наш опыт показывает, что компании долгое время могут не догадываться о том, что ведется атака. Например, до тех пор, пока деструктивные действия не станут заметны: не будут украдены деньги, выведена из строя инфраструктура или оглашена конфиденциальная информация. Следы АРТ-атаки могут тщательно скрываться. Злоумышленники, обладая достаточной мотивацией и временными ресурсами, могут изучить применяемые в компании защитные средства и разработать решение для их обхода. Например, подписать вредоносное ПО сертификатом, чтобы оно выглядело безобидно, использовать легитимные учетные записи, использовать разрешенные в компании средства удаленного доступа, что позволяет максимально замаскироваться под стандартную и легитимную активность, характерную для конкретной компании. Длительное присутствие злоумышленников в инфраструктуре позволяет им заблаговременно получать информацию и о том, какие изменения запланированы в инфраструктуре организации, какие средства защиты пилотируются и внедряются, и, как следствие, — оперативно изменять свой инструментарий таким образом, чтобы они не детектировались обновленными средствами защиты.

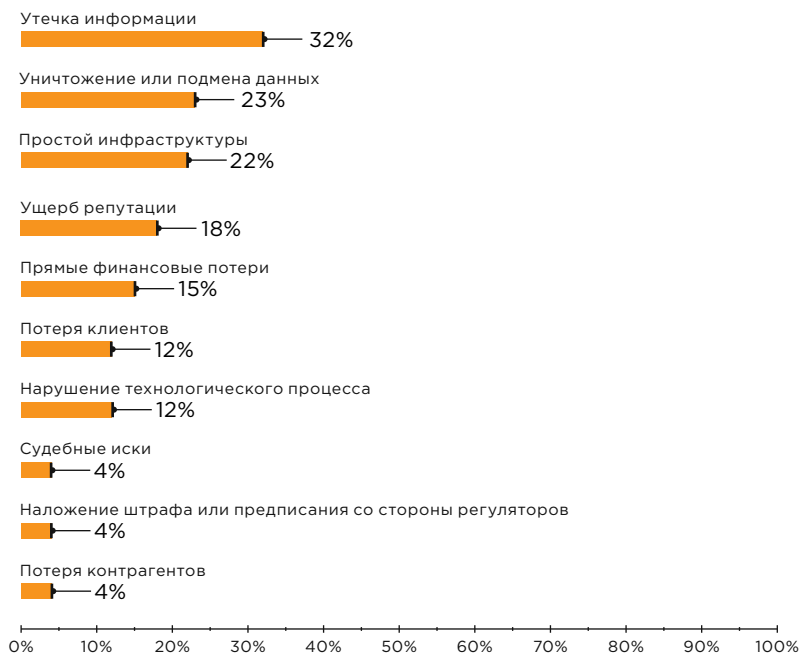
Наибольшее количество респондентов отметило, что столкнулось с угрозой утечки информации. Напомним, что украдены могут быть не только конфиденциальные документы, но и учетные данные сотрудников. Кроме того, компрометация компании может стать промежуточным этапом в сложной схеме злоумышленников и в этом случае целью злоумышленников может быть доступ к почтовому домену (отправка писем от лица компании, spear phishing), к коду программного обеспечения (внесение в код вредоносных скриптов, supply chain attack) и непосредственно к инфраструктуре клиентов или контрагентов (trusted relationship).

В сфере СМБ картина имеет незначительные отличия. Чаще всего компании сталкиваются с утечкой информации, уничтожением и подменой данных (по 32% и 23% соответственно), а также в 22% случаев в качестве последствий от атаки выделен простой инфраструктуры, еще в 18% — ущерб репутации, 15% респондентов отметили в качестве последствия от кибератаки прямые финансовые потери. Потеря клиентов актуальна для 12% опрошенных. Такой же процент приходится на долю нарушения технического процесса. И по 4% столкнулись с такими последствиями, как судебные иски, наложение штрафа или предписания со стороны регулятора, потеря контрагентов. При этом опыт Positive Technologies показывает, что все большую актуальность приобретает сегодня тренд, связанный с атаками на организации через доверенные источники (менее защищенных партнеров, поставщиков, клиентов и пр.), что стирает границы между организациями малого, среднего и крупного бизнеса с точки зрения киберзащищенности. Фишинг такого типа (от лица доверенной организации) входит сегодня в топ-3 наиболее эффективных и часто используемых методов атаки. Например, в течение 2019 года этим способом не брезговали такие группировки, как [TaskMasters](#), [Cobalt](#), [RTM](#), атаковавшие ряд своих целевых организаций от имени (и используя инфраструктуру) организаций-партнеров.



респондентов, работающих в финансовой сфере, отметили, что защита от АРТ-атак является приоритетным направлением развития ИБ в компании

С какими последствиями кибератак сталкивались компании (СМБ)



Отметим, что атаки на IT-компании становятся все более популярны у киберпреступников. Так, по результатам нашего исследования, в ходе которого мы проанализировали поведение двадцати двух АРТ-группировок, атаковавших российские организации на протяжении последних двух лет, 32% атакуют организации, занимающиеся разработкой ПО и системной интеграцией. Порой эти атаки (преимущественно supply chain attack и trusted relationship) – лишь части сложных атак на более серьезные, промышленные или государственные организации или банки.

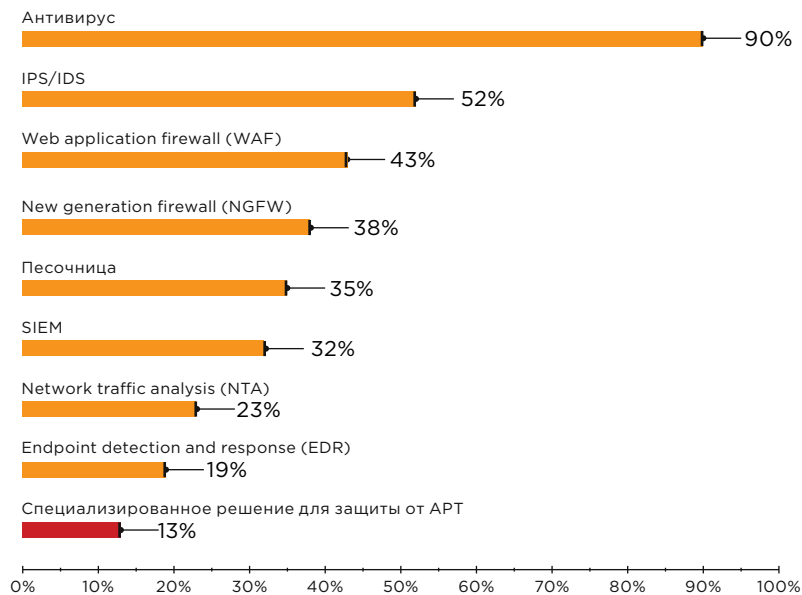
Trusted relationship

атака, в ходе которой злоумышленники используют расширенные права доверенной компании (например, подрядчика, партнера, интегратора) для доступа к инфраструктуре жертвы.

Линия обороны

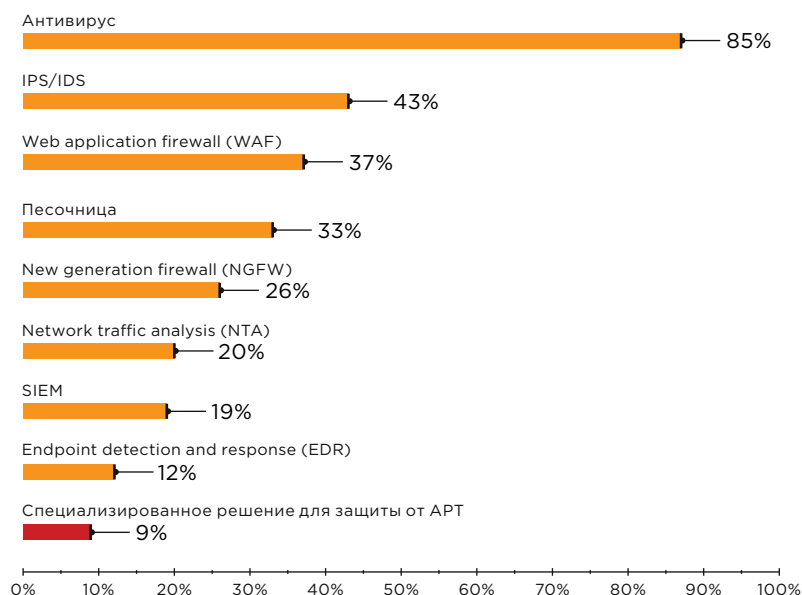
Респонденты привыкли работать с типовыми решениями защиты, внедряемыми в организациях на протяжении многих лет: антивирусами, межсетевыми экранами, IPS/IDS. Мы видим, что вслед за ростом угроз ИБ компании начинают использовать новые технологии для защиты: песочницы, системы глубокого анализа трафика (network traffic analysis), решения для обнаружения, расследования и реагирования на сложные киберугрозы (endpoint detection and response), а также специализированные решения для защиты от АРТ.

Какие технические средства защиты применяются в компаниях (доля респондентов)



При этом если рассматривать только компании СМБ (то есть численностью до 500 сотрудников), то распределение используемых технических средств несколько меняется. На первом месте с 85% остаются антивирусные средства, 43% приходится на долю IPS/IDS, 37% — web application firewall (WAF), 33% — песочницы, на долю решений класса new generation firewall приходится 26%, еще 20% — получают решения класса network traffic analysis, только 19% опрошенных из таких компаний указали использование SIEM-систем, еще 12% — используют endpoint detection and response (EDR) и замыкают рейтинг специализированные решения для защиты от APT (9%).

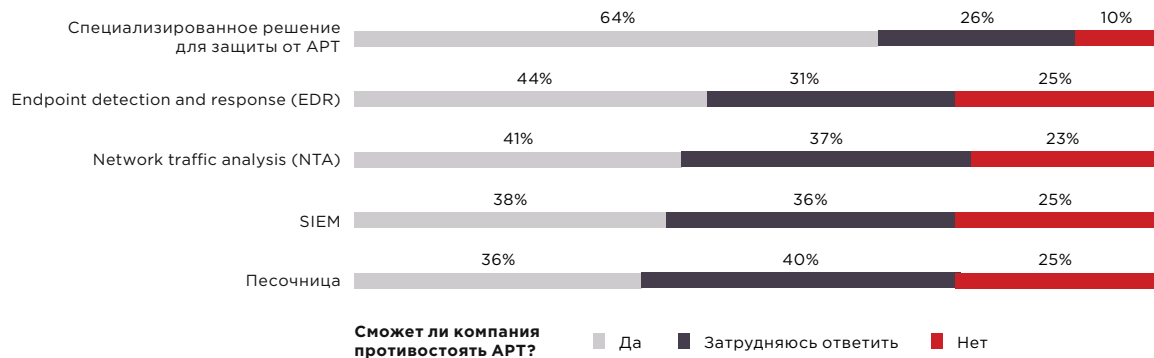
Какие технические средства защиты информации применяются в компании (доля респондентов СМБ)



Результаты опроса показывают, что применение специализированных средств защиты от сложных атак вселяет больше уверенности в сотрудников, что они смогут обнаружить действия АPT-группировки.

Какие технические средства защиты применяются в компании

(доля респондентов, применяющих отдельное средство защиты)

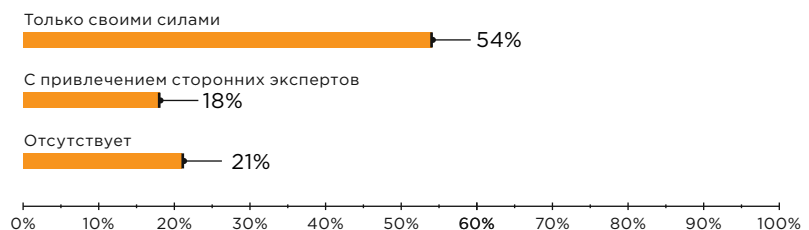


Кадры играют важную роль

Каждый пятый респондент ответил, что в организации отсутствует практика выявления и расследования инцидентов. Зачастую причиной для этого служит отсутствие квалифицированных специалистов или финансовых средств для привлечения сторонних экспертов.

Существует ли в компании практика выявления и расследования киберинцидентов?

(доля респондентов)



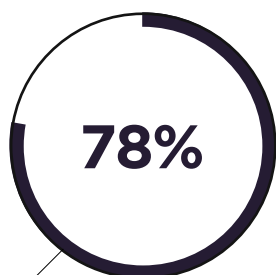
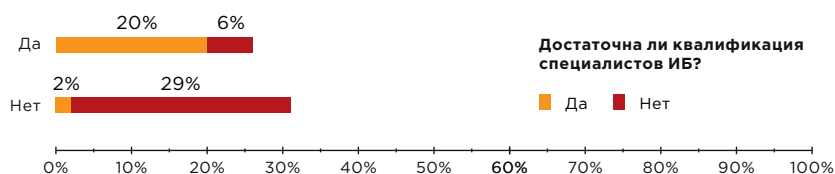
Складывается впечатление, что в большинстве российских компаний считают обучение сотрудников вопросам кибербезопасности формальностью, навязанной требованиями регуляторов. Только 25% респондентов ответили, что тренинги персонала сопровождаются проверкой качества обучения.

Квалификация ИБ-специалистов играет важную роль в противодействии АРТ. Отдельные компоненты обеспечивают защиту от отдельных кибератак, однако сами по себе они не способны справиться с угрозой АРТ. Для выявления, расследования и реагирования на инциденты пока невозможно обойтись только автоматизированными решениями. Специалисты отмечают, что технические средства генерируют большой объем событий безопасности, которые требуют ручной обработки. Кроме того, на плечах ИБ-экспертов лежит приоритизация угроз, реагирование, восстановление систем и расследование инцидентов.

Респонденты считают, что если в компании отсутствуют квалифицированные ИБ-специалисты, то организация вероятнее всего не сможет противостоять АРТ, даже если используются современные технологии защиты.

Сможет ли компания противостоять АРТ

(доля респондентов)



респондентов **не уверены** в готовности компании противостоять АРТ-атаке

для СМБ этот показатель составляет **80%**

Сможет ли компания противостоять АРТ

По результатам исследования мы видим, что сотрудники не уверены в готовности организаций противостоять АРТ. В российских компаниях широко применяются типовые решения для защиты от угроз ИБ, а вот использование специализированных средств для защиты от сложных целенаправленных атак не распространено. Лишь 27% респондентов отметили, что защита от АРТ-атак является приоритетной в компании. Это усугубляется еще и тем, что по мнению сотрудников, ИБ-специалистам не хватает квалификации для противостояния сложным угрозам.

Ответы респондентов наводят нас на мысль, что риск АРТ сегодня воспринимается достаточно серьезно, но сложившийся подход к обеспечению безопасности пока не соответствует новым угрозам со стороны киберпреступников.

На наш взгляд компаниям не стоит ограничиваться внедрением специализированных средств защиты. Многочисленные расследования инцидентов показывают, что злоумышленники могут годами контролировать инфраструктуру жертвы и при этом оставаться незамеченными. Они маскируют свои действия под легитимные процессы и обнаружить это в момент проникновения злоумышленников в сеть организации практически невозможно, на практике выявлять приходится уже свершившуюся атаку. Если вспомнить в этом контексте кейсы, когда целевая организация атакуется через своего менее защищенного партнера (то есть в ряде случаев мы имеем дело с атакой на компанию крупного уровня через СМБ-организацию), то в качестве рекомендации следует упомянуть и необходимость оценки защищенности партнерских организаций. На сегодняшний день такие

требования к защищенности партнерских организаций — ближе к правилам ведения бизнеса, принятых на уровне отдельных организаций. Тем не менее этот подход все чаще оказывается частью мировых стандартов (таких, например, как ISO 27001 или PCI DSS) или даже законодательства отдельных стран (например, Постановление Правительства РФ №127 «Об утверждении Правил категорирования объектов КИИ Российской Федерации, а также перечня показателей критериев значимости объектов КИИ Российской Федерации и их значений» обязывает субъекта КИИ при выборе мер защиты учитывать ситуацию, в которой взломанным оказывается контрагент субъекта). Стремление крупного бизнеса обеспечить непрерывность работы, надежность всех процессов и, конечно, повысить свою киберзащищенность в целом, логичным образом в обозримом будущем приведут к росту требований с точки зрения ИБ в отношении компаний рынка СМБ (для которых в какой-то момент способность противостоять кибератакам может превратиться в конкурентное преимущество).

Регулярный ретроспективный анализ и перепроверка почтовых вложений и других файлов с использованием вновь полученных индикаторов компрометации позволяют обнаружить артефакты, указывающие на киберпреступников. Например, сегодня может появиться сигнатура на то ВПО, которое хакеры использовали в атаке неделю назад. Этого времени может быть достаточно, чтобы расследовать инцидент и устранить угрозу до того, как злоумышленники доберутся до критически важных активов компании.

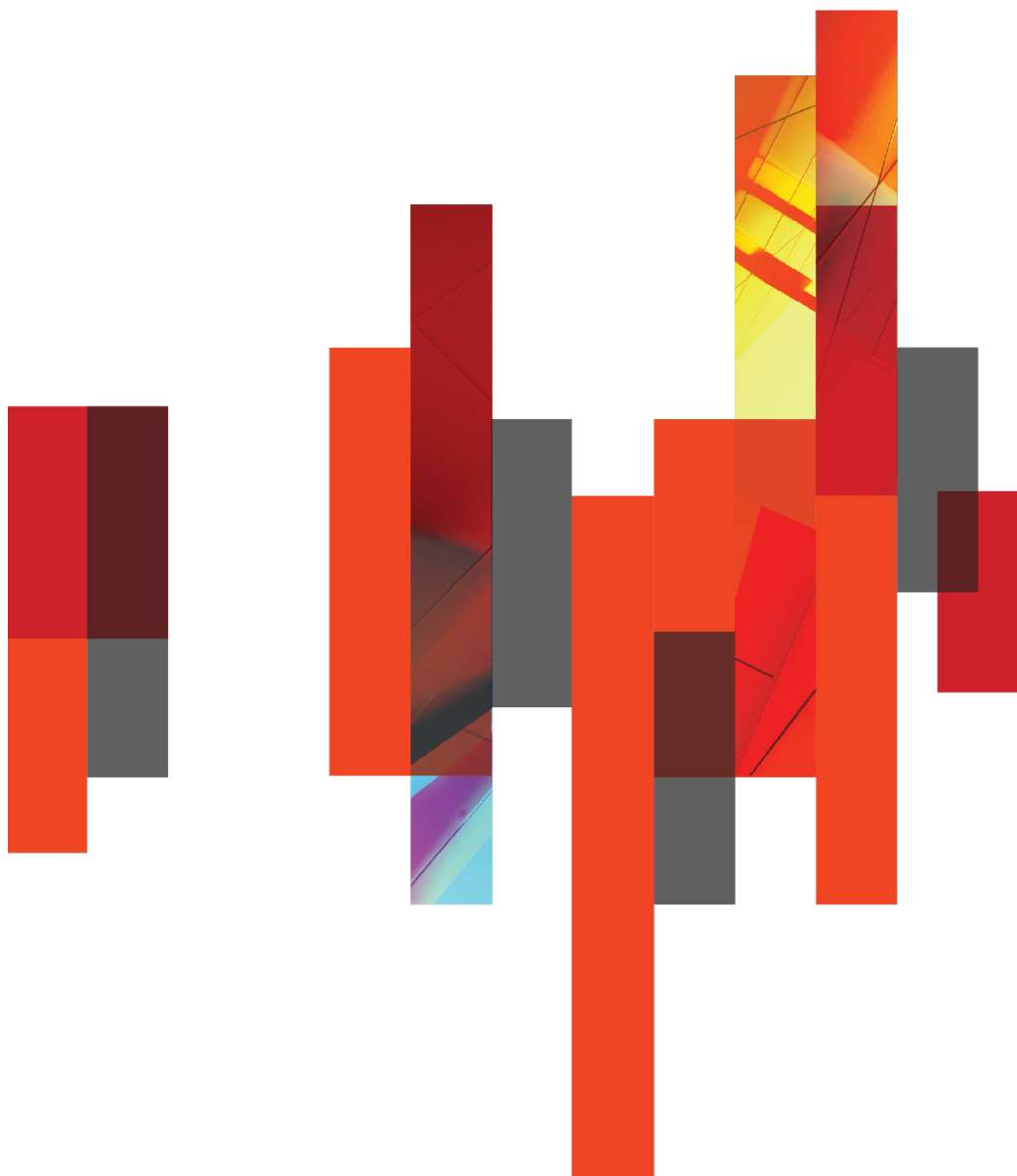
Второй момент — это наличие квалифицированных кадров для выполнения большого объема работ:

- настройка и контроль функционирования технических средств защиты;
- сбор и обработка информации о событиях безопасности;
- анализ трафика и поиск подозрительной активности в инфраструктуре;
- реагирование на инциденты и восстановление систем.

В случае отсутствия или нехватки квалифицированных специалистов в штате компании часть задач лучше переложить на внешних специалистов, обладающих более глубокими знаниями в области анализа киберугроз.

Как защититься?

Рекомендации от Microsoft
и Positive Technologies



Как защититься, если вы обычный пользователь?

Не экономьте на безопасности:

- используйте только лицензионное ПО;
- используйте эффективные средства антивирусной защиты на всех устройствах;
- своевременно обновляйте используемое ПО по мере выхода патчей.

Защищайте ваши данные:

- наиболее важные файлы храните не только на жестком диске компьютера, но и на съемных носителях, внешних жестких дисках или в облачном хранилище;
- для повседневной работы в ОС используйте учетную запись без привилегий администратора;
- используйте многофакторную аутентификацию там, где это возможно, например для защиты электронной почты. Причем подтверждение по СМС не является предпочтительным методом.

Не используйте простые пароли:

- используйте сложные пароли, состоящие из незначущих комбинаций букв, цифр и знаков, длиной не менее 8 символов. Для создания и хранения паролей можно воспользоваться менеджером паролей (защищенным хранилищем с функциями генерации новых паролей);
- не используйте один и тот же пароль для разных систем (для сайтов, электронной почты и др.);
- меняйте все пароли хотя бы раз в полгода, а лучше — каждые два-три месяца.
- современный тренд — полный отказ от паролей в пользу средств многофакторной аутентификации

Будьте бдительны:

- проверяйте все вложения, полученные по электронной почте, с помощью антивирусного ПО;
- с осторожностью относитесь к сайтам с некорректными сертификатами и учитывайте, что введенные на них данные могут быть перехвачены злоумышленниками;
- будьте предельно внимательны при вводе учетных данных на сайтах и во время работы с онлайн-платежами;
- не переходите по ссылкам на незнакомые подозрительные ресурсы, особенно когда браузер предупреждает об опасности;
- не переходите по ссылкам из всплывающих окон, даже если рекламируемые компания или продукт вам знакомы;
- не загружайте файлы с подозрительных веб-ресурсов или из других неизвестных источников.



Как защититься, если вы организация?

Используйте эффективные технические средства защиты:

- системы централизованного управления обновлениями и патчами для используемого ПО. Для правильной приоритизации планов по обновлениям необходимо учитывать сведения об актуальных угрозах безопасности.
- системы антивирусной защиты со встроенной изолированной средой («песочницей») для динамической проверки файлов, способные выявлять и блокировать вредоносные файлы в корпоративной электронной почте до момента их открытия сотрудниками и другие вирусные угрозы. Наиболее эффективным будет использование антивирусного ПО, построенного на решениях одновременно нескольких производителей, способного обнаруживать скрытое присутствие вредоносных программ и позволяющего выявлять и блокировать вредоносную активность в различных потоках данных — в почтовом, сетевом и веб-трафике, в файловых хранилищах, на веб-порталах. Важно, чтобы выбранное решение позволяло проверять файлы не только в реальном времени, но и автоматически анализировало уже проверенные ранее, это позволит выявить не обнаруженные ранее угрозы при обновлении баз сигнатур.
- SIEM-решения — для своевременного выявления и эффективного реагирования на инциденты информационной безопасности. Это позволит своевременно выявлять злонамеренную активность, попытки взлома инфраструктуры, присутствие злоумышленника и принимать оперативные меры по нейтрализации угроз.
- автоматизированные средства анализа защищенности и выявления уязвимостей в ПО.
- межсетевые экраны уровня приложений (web application firewalls) — в качестве превентивной меры защиты веб-ресурсов.
- системы глубокого анализа сетевого трафика — для обнаружения сложных целевых атак как в реальном времени, так и в сохраненных копиях трафика. Применение такого решения позволит не только увидеть не обнаруженные ранее факты взлома, но и в режиме реального времени отслеживать сетевые атаки, в том числе запуск вредоносного ПО и хакерских инструментов, эксплуатацию уязвимостей ПО и атаки на контроллер домена. Такой подход позволит существенно снизить время скрытного присутствия нарушителя в инфраструктуре, и тем самым минимизировать риски утечки важных данных и нарушения работы бизнес-систем, снизить возможные финансовые потери от присутствия злоумышленников.
- специализированные сервисы анти-DDoS.

Защищайте данные:

- не храните чувствительную информацию в открытом виде или в открытом доступе;
- регулярно создавайте резервные копии систем и храните их на выделенных серверах отдельно от сетевых сегментов рабочих систем;
- минимизируйте, насколько это возможно, привилегии пользователей и служб;
- используйте разные учетные записи и пароли для доступа к различным ресурсам;
- применяйте двухфакторную аутентификацию там, где это возможно, например для защиты привилегированных учетных записей.

Не допускайте использования простых паролей:

- применяйте парольную политику, предусматривающую строгие требования к минимальной длине и сложности паролей;
- ограничьте срок использования паролей (не более 90 дней);
- смените стандартные пароли на новые, удовлетворяющие строгой парольной политике;
- современный тренд — полный отказ от паролей в пользу средств многофакторной аутентификации.

Контролируйте безопасность систем:

- своевременно обновляйте используемое ПО по мере выхода патчей;
- проверяйте и повышайте осведомленность сотрудников в вопросах информационной безопасности;
- контролируйте появление небезопасных ресурсов на периметре сети; регулярно проводите инвентаризацию ресурсов, доступных для подключения из интернета; анализируйте защищенность таких ресурсов и устраняйте уязвимости в используемом ПО; хорошей практикой является постоянный мониторинг публикаций о новых уязвимостях: это позволяет оперативно выявлять такие уязвимости в ресурсах компании и своевременно их устранять;
- эффективно фильтруйте трафик для минимизации доступных внешнему злоумышленнику интерфейсов сетевых служб; особое внимание стоит уделять интерфейсам удаленного управления серверами и сетевым оборудованием;
- регулярно проводите тестирование на проникновение для своевременного выявления новых векторов атак на внутреннюю инфраструктуру и оценки эффективности принятых мер по защите;
- регулярно проводите анализ защищенности веб-приложений, включая анализ исходного кода, с целью выявления и устранения уязвимостей, позволяющих проводить атаки, в том числе на клиентов приложения;
- отслеживайте количество запросов к ресурсам в секунду, настройте конфигурацию серверов и сетевых устройств таким образом, чтобы нейтрализовать типичные сценарии атаки (например, TCP- и UDP-флуд или множественные запросы к БД).

Запустите программу повышения осведомленности сотрудников в области ИБ (Awareness):

- регулярно напоминайте о правилах безопасной работы в интернете, разъясняйте методы атак и способы защиты;
- предостерегайте сотрудников от ввода учетных данных на подозрительных веб-ресурсах и тем более от сообщения такой информации кому бы то ни было по электронной почте или во время телефонного разговора;
- разъясняйте порядок действий в случае подозрений о мошенничестве;
- уведомляйте о событиях, связанных с информационной безопасностью;
- проводите тренинги для сотрудников по вопросам ИБ, с последующей проверкой эффективности;
- научите сотрудников оповещать своих «безопасников» о том, что им пришло фишинговое письмо, особенно если заметно, что над рассылкой тщательно поработали. В таком случае, даже если заражение или утечка имели место, еще можно успеть оперативно отреагировать на атаку и принять контрмеры.

О составителях

Microsoft (Nasdaq «MSFT» @microsoft) обеспечивает условия для цифровой трансформации в эпоху «интеллектуального облака» и «интеллектуальных технологий». Миссия компании — дать возможность каждому человеку и организации на планете достичь большего.

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

Аналитики TAdviser с 2005 года провели десятки исследований в интересах заказчиков и поставщиков IT-систем. В течение многих лет TAdviser формирует уникальную базу проектов российских компаний из 37 отраслей экономики по внедрению информационных систем различных поставщиков. Среди клиентов: ГИВЦ Москвы, ФСК ЕЭС, «Энергодата», Baltischug Kempinski, «Спортмастер», Stockmann, «Самохвал», «Бахетле», «Русский Стандарт Страхование», SAP, Microsoft, Oracle, «Ситроникс», IBS, R-Style, Abbyy, SAS Institute, «РДТех», QlikTech, «Галактика», «Техносерв», «БДО Юникон», «Энвижн Груп», «АйТи» и многие другие организации.