2014

Информационная безопасность бизнеса

Исследование текущих тенденций в области информационной безопасности бизнеса

kaspersky.ru/business

KASPERSKY lab

СОДЕРЖАНИЕ

Введение 2
Основные цифры 3
География опроса 4
Приоритеты IT-менеджеров 5
Риски информационной безопасности: инциденты и меры 7
Применяемые методы защиты 8
Инциденты IT-безопасности: внешние угрозы 9
Оценка потерь от внешних угроз 10
Инциденты IT-безопасности: внутренние угрозы 11
Оценка потерь от внутренних угроз 12
Оценка последствий: 20 миллионов рублей за один инцидент 13
Дополнительные расходы, вызванные инцидентом ИБ 14
Утечки данных: опасения и реальность 15
Виртуализация 16
Информационная безопасность в сегменте среднего и малого бизнеса 17
Заключение: важность выбора подходящей защиты 18

ВВЕДЕНИЕ

«Лаборатория Касперского» является крупнейшей в мире частной компанией, занимающейся разработкой защитных решений для домашних пользователей и корпоративных IT-инфраструктур. Чтобы всегда предоставлять своим клиентам надежную и отвечающую их потребностям защиту, компания регулярно проводит специализированные исследования, позволяющие выявить главные риски и угрозы, которые беспокоят представителей бизнеса.

С 2011 года «Лаборатория Касперского» совместно с международной аналитической компанией B2B International проводит ежегодный глобальный опрос IT-специалистов малых, средних и крупных компаний по всему миру. Исследование позволяет узнать мнение этих профессионалов относительно самых важных вопросов безопасности корпоративной IT-инфраструктуры: о корпоративном защитном программном обеспечении, об уровне осведомленности о киберугрозах, а также о том, с какими проблемами в области кибербезопасности чаще всего приходится сталкиваться компаниям, как они эти проблемы решают и чего ожидают в этой сфере в будущем.

Сравнение новых данных с теми, что были получены в предыдущие годы, позволяет выявить тенденции, характерные для исследуемой области, и проанализировать их, что в конечном итоге дает максимально полную и, по нашему мнению, объективную картину ландшафта угроз, проблем и перспектив в сфере информационной безопасности бизнеса. Ниже приведены результаты опроса российских компаний.

ОСНОВНЫЕ ЦИФРЫ

По итогам опроса, главными в сфере угроз информационной безопасности и противодействия им стали следующие тенденции:

- 41% компаний отметили как главный приоритет защиту конфиденциальных данных от целевых атак;
- 91% компаний недооценивают количество существующего вредоносного ПО;
- Антивирусное ПО остается наиболее распространенной мерой обеспечения информационной безопасности в организациях;
- В течение года 98% предприятий столкнулись с инцидентами кибербезопасности, источники которых находились за пределами компании, что на 3% больше, чем годом ранее. Четверть компаний потеряли данные в результате внешних кибератак;
- 87% компаний пострадали от внутренних угроз; почти четверть (24%) таких инцидентов привели к потере конфиденциальных данных;
- Ущерб от одного инцидента информационной безопасности в среднем составляет около 20 млн. рублей для крупной компании и свыше 780 тыс. рублей для компании сегмента СМБ;
- На ликвидацию последствий инцидента и профилактику крупные компании дополнительно тратят около 2,1 млн. руб., а небольшие – около 300 тыс. рублей;
- Чаще всего в результате инцидентов кибербезопасности компании теряют операционные данные о внутренней деятельности, персональные данные клиентов и финансовые сведения.

О том, как российский бизнес видит современные киберугрозы, читайте далее.

ГЕОГРАФИЯ ОПРОСА

Отчет подготовлен по итогам интервью 3900 респондентов – представителей компаний из 27 стран мира, включая Россию (Центральный, Южный, Северо-Западный, Дальневосточный, Северо-Кавказский, Сибирский, Уральский и Приволжский федеральные округа). Все участники опроса имеют влияние на формирование политики своих компаний в области IT и обладают знаниями в отношении как рисков информационной безопасности, так и функционирования других бизнес-подразделений компании. В опросе представлено мнение сотрудников предприятий малого и среднего бизнеса, а также крупных корпораций. Период исследования охватывает 12 месяцев, прошедших с апреля 2013 по май 2014 года.

ПРИОРИТЕТЫ IT-МЕНЕДЖЕРОВ

Значительные изменения произошли в тройке самых приоритетных задач в области IT по сравнению с прошлым годом: главной проблемой 41% респондентов назвал защиту конфиденциальных данных (данных о клиентах, финансовой информации и др.) от целевых атак, которая в прошлом году даже не входила в этот список. На второе место (34%) переместился более общий вопрос защиты данных, который лидировал до этого на протяжении трех лет. А третье место получила задача, ранее также не попадавшая в список приоритетных: 29% опрошенных отметили необходимость обеспечения бесперебойной работы критически важных систем (например, за счет применения средств защиты от DDoS-атак).

Причинами роста внимания IT-менеджмента к данным задачам мог послужить ряд громких целевых атак, имевших место в прошедшем году. Так, за период исследования «Лаборатория Касперского» раскрыла три крупные кибершпионские кампании, целью которых было похищение секретных данных корпораций и государственных организаций по всему миру. Примером того, какими разрушительными могут быть последствия целевой атаки, стало нападение киберпреступников на крупного ритейлера Target, в результате чего в руки злоумышленников попали персональные данные около 70 миллионов клиентов этого популярного магазина.

Защита от целевых атак является приоритетной, прежде всего, для среднего бизнеса (43%) и крупных предприятий (38%), в то время как малый бизнес этот вопрос волнует заметно меньше – только 32% его представителей относят защиту от целевых атак к своим ключевым задачам.

Рост внимания к вопросу обеспечения непрерывности бизнес-процессов в случае DDoS-атак также может быть следствием недавних громких событий. Так, во время весенней «кампании» злоумышленников, избравших в качестве своей мишени сразу несколько ведущих российских банков, крупных компаний и государственных учреждений, «Лаборатория Касперского» зафиксировала новый скачок мощности DDoS-атак в Рунете. Средняя мощность атаки составляла 70-80 Гб/с, а в пиковые моменты превышала 100 Гб/с. Такие показатели стали новым рекордом для российского сегмента Глобальной сети — всего год назад самая мощная DDoS-атака в Рунете не превышала порога в 60 Гб/с.

ПРИОРИТЕТЫ IT-МЕНЕДЖЕРОВ

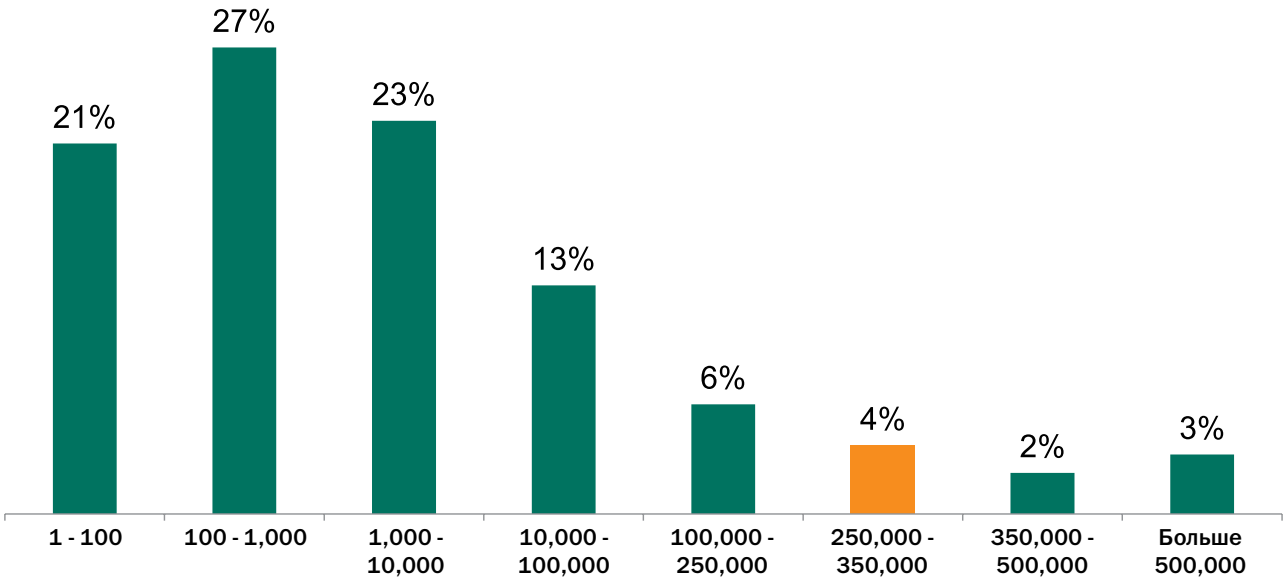
Особенно любопытно выглядит распределение подзадач внутри пункта «**Управление изменениями в IT-системах и инфраструктуре**». Рассмотрим его подробнее:

Среди наиболее важных задач, связанных с управлением IT-инфраструктурой компании, на первое место в 2014 году вышел вопрос развертывания виртуальных серверов и рабочих станций – такой ответ дала ровно половина респондентов. Стремление оптимизировать расходы на масштабирование и обслуживание IT-инфраструктуры приводит все больше компаний к выбору решений на базе технологий виртуализации. Однако вместе с преимуществами, которые несет виртуализация, приходят и сложности, связанные, в том числе, с безопасностью – лишь 18% представителей российских компаний отметили, что полностью обеспечили защиту виртуальных сред. Еще 65% внедрили средства защиты частично, а в 14% компаний не применяются никакие специальные инструменты защиты.

Вслед за виртуализацией перед IT-менеджментом остро стоит задача частичного обновления оборудования – ее отметили 47% респондентов, а еще 45% заявили о необходимости внедрения в их компаниях нового программного обеспечения.

РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ИНЦИДЕНТЫ И МЕРЫ

Знание современных темпов развития киберугроз является косвенным показателем того, насколько эффективно компания может противостоять атакам. Чтобы выяснить уровень осведомленности российских компаний, «Лаборатория Касперского» второй год подряд просит респондентов оценить количество нового вредоносного ПО, которое появляется ежедневно.



Оценка количества ежедневно появляющегося вредоносного ПО

Ежедневно эксперты «Лаборатории Касперского» обрабатывают в среднем 315 тысяч образцов вредоносного ПО. Однако в ходе опроса лишь 4% респондентов назвали сходную цифру, в то время как 91% ее занизили. Примечательно, что в этом году 5% опрашиваемых переоценили угрозу, что не было характерно для российских компаний ранее.

Оценка уровня опасности неизбежно влияет на то, какие меры принимают компании для защиты от киберугроз.

ПРИМЕНЯЕМЫЕ МЕТОДЫ ЗАЩИТЫ

60% респондентов сообщили, что в течение исследуемого периода на рабочих станциях, используемых в их компаниях, было установлено защитное ПО. Этот показатель существенно (на 14 п.п.) ниже, чем по итогам прошлогоднего опроса. Также снизилась популярность такой меры защиты, как регулярное обновление ПО и установка обновлений (патчей) – ее уровень достиг 53%, упав на 6 п.п. Контроль приложений вырос на 6 п.п. по популярности и расположился на третьем месте (38%).

Еще одно существенное снижение показателей коснулось шифрования информации на рабочих станциях сотрудников компании – соответствующие инструменты начали использовать 23% организаций (против 33% годом ранее).

Все эти изменения обусловлены несколькими факторами, один из которых – сравнительно высокий уровень распространенности указанных мер информационной безопасности в компаниях. И антивирусное ПО, и обновление программ, и системы шифрования данных уже несколько лет входят в состав стандартного набора средств информационной безопасности, используемых в российских компаниях. Их уровень проникновения высок и, соответственно, все меньше респондентов опроса включают их в список мер, впервые принятых за исследуемый период.

Среди новых для 2014 года мер, принятых компаниями для обеспечения информационной безопасности, – внедрение систем для защиты финансовых транзакций (36% респондентов), технологий защиты мобильных устройств (31%), а также средств поддержания работоспособности веб-сервисов и защиты от DDoS-атак (28%). Кроме того, почти четверть (24%) респондентов отметили в качестве новой меры безопасности применение систем для защиты от утечек данных (Data Leakage Protection, DLP).

В целом результаты опроса показывают, что большинство компаний рассматривают антивирусное ПО как основное средство для обеспечения информационной безопасности, а компании, признающие необходимость использования дополнительных средств, таких как MDM-системы или средства защиты от утечек и перехвата критически важной бизнес-информации, пока в меньшинстве. Эта тенденция сохраняется уже много лет, в то время как ландшафт киберугроз постоянно меняется.

ИНЦИДЕНТЫ IT-БЕЗОПАСНОСТИ: ВНЕШНИЕ УГРОЗЫ

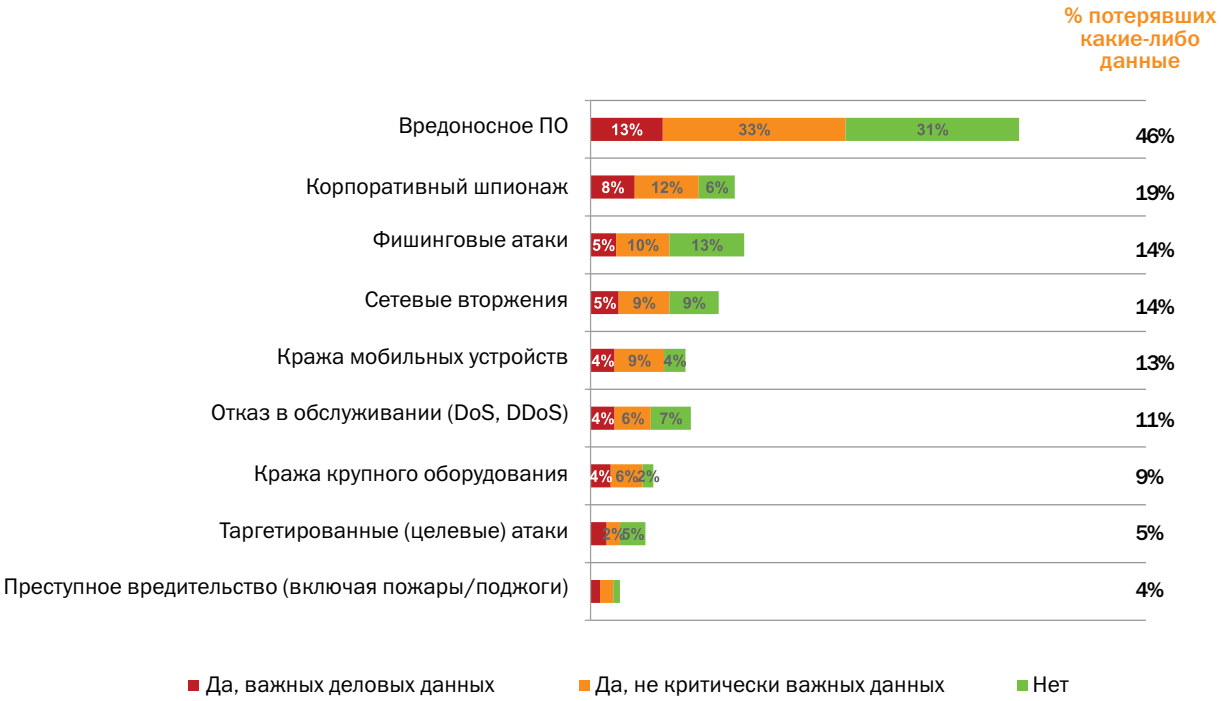
Компании любого размера в любой стране мира регулярно сталкиваются с инцидентами информационной безопасности. В России этот показатель ежегодно увеличивается и, более того, приближается к 100%: по результатам опроса, за последние 12 месяцев 98% российских компаний столкнулись хотя бы с одним инцидентом информационной безопасности, вызванным внешними факторами. За год количество компаний, подвергавшихся внешним кибератакам, выросло на 3 п.п.

Самой значимой среди внешних угроз (77%) по-прежнему является вредоносное ПО. Лишь на 3% отстают нежелательные электронные письма (74%), а ведь именно в спаме часто содержатся вирусы или ссылки на фишинговые сайты. Кстати, фишинговые атаки стали в этом году третьей по значимости внешней угрозой – с ними столкнулись 28% российских компаний.

Важно отметить рост на 5 п.п. (с 13% до 18%) количества DDoS-атак: в октябре 2013 года группа хакеров провела атаку на несколько ключевых российских банков, а весной 2014 года хакерскими организациями, такими как Anonymous Caucasus, была совершена серия мощных DDoS-атак на СМИ, различные государственные и окологосударственные сервисы.

В этом году сильно выросла доля корпоративного шпионажа – в основном за счет сильного увеличения количества таких инцидентов в крупных организациях (почти треть компаний, 32%). В СМБ-сегменте этот показатель существенно ниже – 19%. По всем остальным пунктам внешние угрозы также демонстрируют тенденцию к росту.

ОЦЕНКА ПОТЕРЬ ОТ ВНЕШНИХ УГРОЗ



Одним из основных последствий успешной кибератаки, вне зависимости от ее типа, становится потеря атакованной организацией важной информации. В этом году успешность внешних атак выросла на 5 п.п.: четверть респондентов сообщили, что теряли данные за последние 12 месяцев.

Атаки с использованием вредоносного ПО являются не только самыми распространенными, но и самыми опасными: они приводили к утечке бизнес-информации в 46% случаев. Еще в 19% случаев потери данных происходили в результате промышленного шпионажа, и в 14% случаев компании теряли информацию из-за фишинговых атак.

Вместе с тем, внешние угрозы – далеко не единственная проблема IT-безопасности, с которой приходится иметь дело современным компаниям. Не меньший вред способны нанести бизнесу угрозы внутренние.

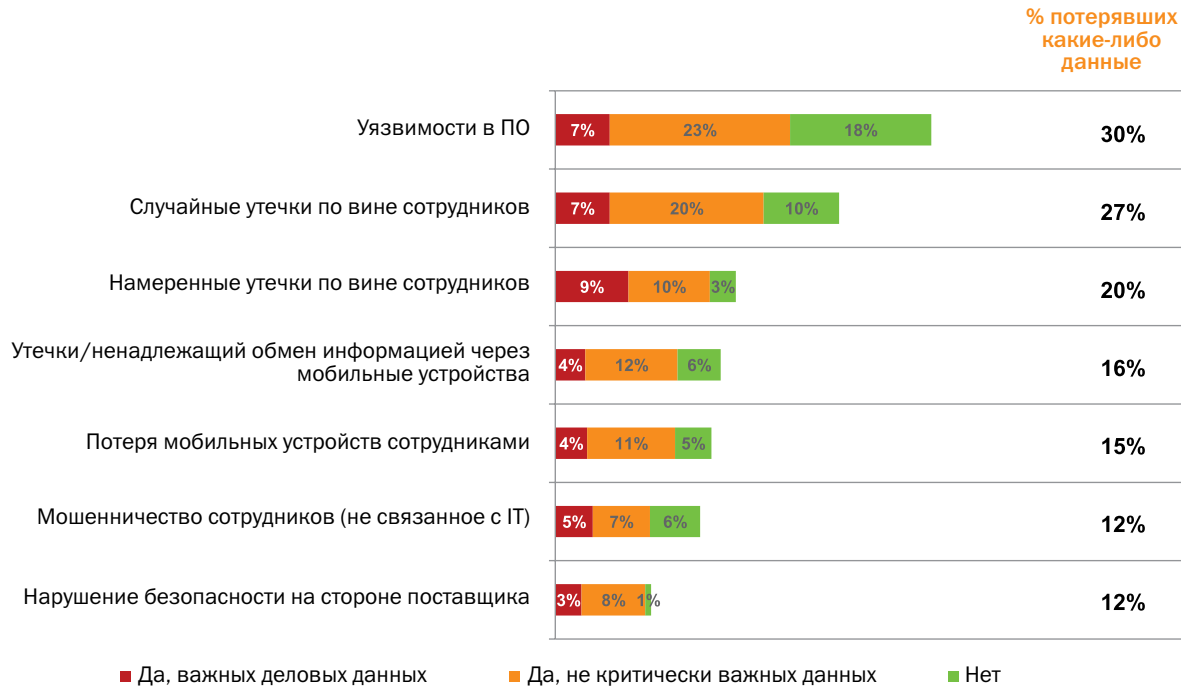
ИНЦИДЕНТЫ IT-БЕЗОПАСНОСТИ: ВНУТРЕННИЕ УГРОЗЫ

Как и в прошлом году, ключевыми рисками внутри компаний являются уязвимости в ПО (48%), незнание сотрудниками правил IT-безопасности, приводящее к случайным утечкам данных (36%), а также намеренное раскрытие конфиденциальной информации сотрудниками (23%).

Позитивным сигналом является тот факт, что количество респондентов, сообщающих об уязвимостях в корпоративном ПО, планомерно сокращается. В 2011 году, когда этот опрос проводился впервые, 65% компаний сообщили об инцидентах, связанных с этой угрозой. По сравнению с 2013 годом результаты нового опроса ниже на 3 п.п., что может быть следствием использования решений для управления обновлениями программного обеспечения.

Примечательно, что от трех самых распространенных внутренних угроз СМБ-компании страдают меньше, чем крупный бизнес: лишь 44% (против 52%) столкнулись с уязвимостями в ПО, в 28% небольших компаний (против 40% корпораций) произошли утечки данных из-за неосторожности сотрудников, и в 19% (против 26%) сотрудники действовали злонамеренно.

ОЦЕНКА ПОТЕРЬ ОТ ВНУТРЕННИХ УГРОЗ



Разумеется, все эти типы угроз приводили к потере компаниями секретной информации. В среднем в результате внутренних инцидентов информационной безопасности лишились конфиденциальных сведений около 24% организаций.

Самыми опасными инцидентами в плане кражи любого типа данных являются уязвимости в ПО и случайные утечки информации – от них пострадали 30% и 27% компаний соответственно. Однако намеренные действия сотрудников приводят к более серьезным последствиям: по этой причине произошло 20% случаев утечек данных, и в 9% случаев инсайдеры похитили критически важную для бизнеса информацию. Для инцидентов, вызванных другими причинами, показатель потери критически важных данных гораздо ниже – от 3% до 7%.

Ландшафт внешних и внутренних угроз, с которыми столкнулись компании за последние 12 месяцев, наглядно демонстрирует необходимость использования комплексных защитных решений. Сам факт наличия подобных инцидентов также указывает на то, что пока IT-инфраструктура компаний защищена недостаточно хорошо. У этой ситуации множество причин, в том числе недостаточно адекватная оценка уровня угрозы и другие факторы, такие как убежденность в том, что финансовый ущерб от кибератаки в любом случае будет ниже, чем инвестиции в приобретение и развертывание защитных решений.

Между тем, как показали результаты опроса, ущерб, причиненный кибератакой, может значительно превышать бюджеты многих компаний, выделяемые на обеспечение информационной безопасности.

ОЦЕНКА ПОСЛЕДСТВИЙ: 20 МИЛЛИОНОВ РУБЛЕЙ ЗА ОДИН ИНЦИДЕНТ

Кибератаки приводят к значительным финансовым потерям. Этот тезис уже второй год подтверждается результатами опроса, проводимого B2B International и «Лабораторией Касперского». Как и в прошлом году, при оценке финансового ущерба от кибератак эксперты опросили представителей компаний, которые столкнулись с утечкой конфиденциальных данных в результате инцидента информационной безопасности.

Респондентам задавали вопросы как о прямых финансовых убытках в результате кибератаки, так и о дополнительных расходах, которые пришлось понести атакованной компании. При этом учитывались ответы тех участников опроса, которые имели право разглашать конкретную цифру убытков, понесенных компанией в результате атаки.

Используя полученные данные об убытках и расходах на дополнительные услуги, к которым компании были вынуждены прибегнуть после атаки на свою IT-инфраструктуру, а также среднюю цену на подобные услуги на рынках разных стран, была рассчитана средняя сумма финансового ущерба, который несут компании, подвергшиеся кибератакам.

Убытки от инцидента складываются из расходов на профессиональные сервисы (внешние специалисты по информационной безопасности, юристы, специалисты по связям с общественностью и т.д.), упущенных бизнес-возможностей (испорченная репутация, срыв контрактов из-за инцидента и т.п.), а также ущерба от вынужденного простоя IT-инфраструктуры компании и приостановки бизнес-процессов.

В результате выяснилось, что в среднем от одного инцидента информационной безопасности крупные компании теряют около 20 млн. рублей, а компании сегмента СМБ – около 780 тыс. рублей. За прошедший год сумма средних потерь для небольших компаний выросла более чем на 100 тыс. рублей, в то время как для крупных компаний она снизилась.

Средний ущерб
для СМБ-компаний
от серьезного инцидента

780 тыс. руб.

Средний ущерб
для крупных предприятий
от серьезного инцидента

20 млн. руб.

Для расчета среднего ущерба оценивались следующие параметры: затраты на услуги внешних специалистов, упущенные бизнес-возможности, остановка бизнес-процессов (простой)

ДОПОЛНИТЕЛЬНЫЕ РАСХОДЫ, ВЫЗВАННЫЕ ИНЦИДЕНТОМ ИБ

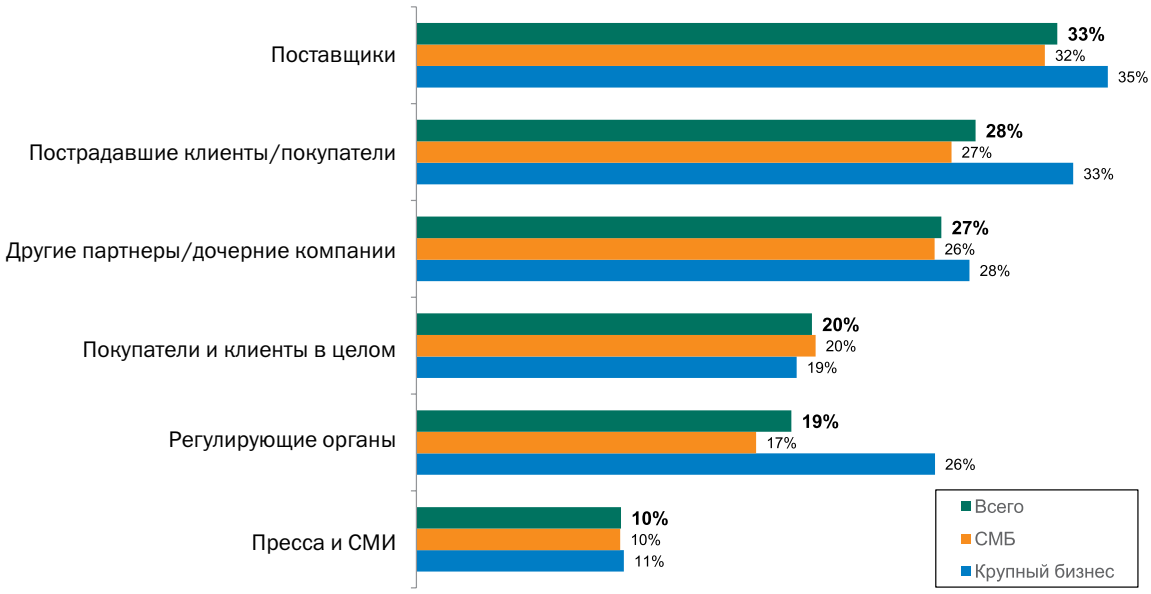
Значительную часть суммы, которую теряет компания в результате серьезного инцидента информационной безопасности, составляют дополнительные расходы на устранение последствий инцидента и предотвращение подобных происшествий в будущем.

СМБ
Средние расходы

Крупные компании
Средние расходы

Общая оценка дополнительных затрат складывается из расходов на подбор дополнительного персонала, проведение тренингов по информационной безопасности для сотрудников и приобретение программного обеспечения и аппаратуры для защиты информационных систем компании от внешних и внутренних инцидентов в будущем. Для средних и малых компаний эти расходы составляют около 324 тыс. рублей, для крупных – около 2,2 млн. рублей.

РЕПУТАЦИОННЫЕ ПОТЕРИ: КОМУ АТАКОВАННЫЕ КОМПАНИИ БЫЛИ ВЫНУЖДЕНЫ РАСКРЫТЬ ИНФОРМАЦИЮ ОБ ИНЦИДЕНТЕ



Процент компаний, которые были вынуждены раскрыть информацию третьим сторонам

Помимо финансовых потерь, инцидент информационной безопасности приводит к репутационному ущербу. Так, за исследуемый период 59% компаний были вынуждены публично признать произошедшее и раскрыть конфиденциальную информацию. В 33% случаев компания уведомляла клиентов, которые могли пострадать в результате инцидента, в 28% случаев – партнеров, и в 27% – поставщиков.

Крупные корпорации в большинстве случаев обязаны сообщить об инциденте регулятору, клиентам и прессе, что наносит серьезный удар по деловой репутации таких компаний.

УТЕЧКИ ДАННЫХ: ОПАСЕНИЯ И РЕАЛЬНОСТЬ

Одним из самых болезненных последствий инцидента безопасности является утечка данных. Давайте сравним статистику данных, которые чаще всего крадут злоумышленники, и данных, которые компании больше всего боятся потерять.

ВИДЫ ДАННЫХ, КОТОРЫЕ ЧАЩЕ ВСЕГО КРАДУТ ЗЛОУМЫШЛЕННИКИ

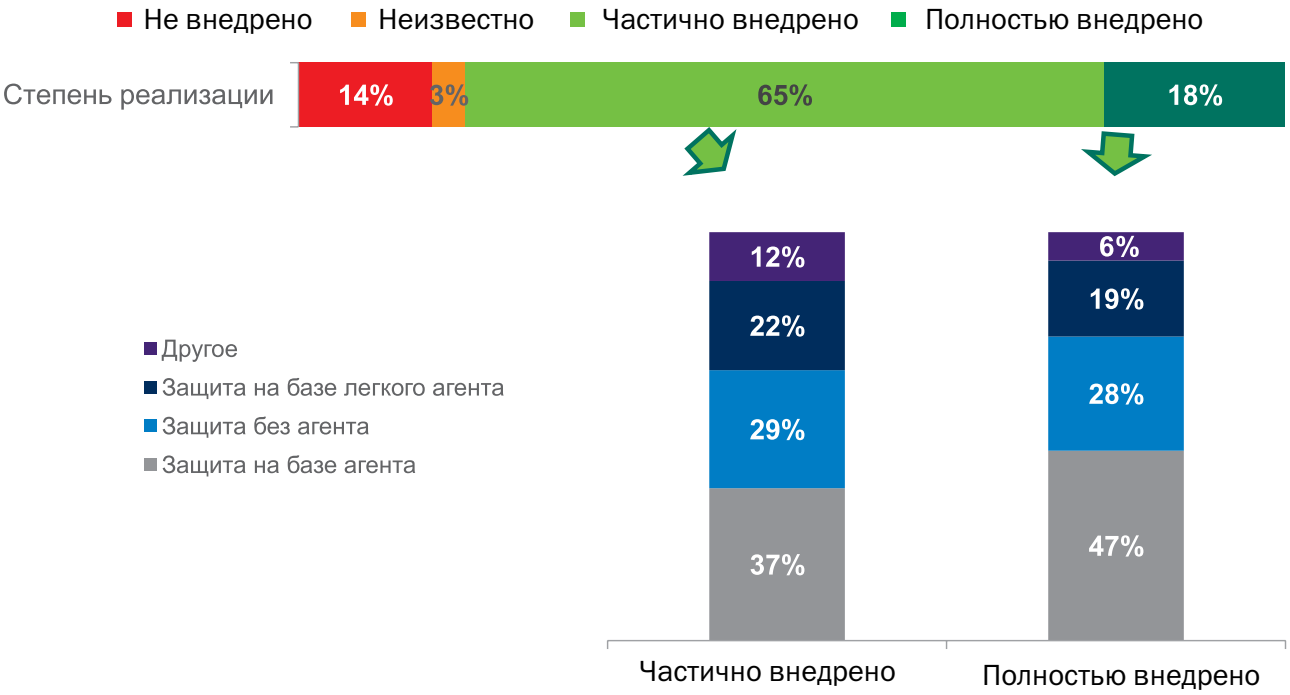
Чаще всего в результате инцидента компании расставались со своей внутренней операционной информацией – об этом сообщили 56% опрашиваемых. На втором месте по частоте утечек (26%) – персональные данные сотрудников, что чревато санкциями со стороны регуляторов. Кражу финансовой информации и данных о клиентах отметили по 25% респондентов соответственно.

ВИДЫ ДАННЫХ, КОТОРЫЕ КОМПАНИИ БОЛЬШЕ ВСЕГО БОЯТСЯ ПОТЕРЯТЬ

Вполне логично, что российские компании больше всего дорожат своими клиентскими базами и прочей информацией о клиентах и заказчиках – эти данные боится потерять 21% организаций. Еще 19% опасаются кражи финансовой информации, и лишь 15% – внутренней операционной информации, которую в реальности крадут чаще всего.

В целом результаты этой части опроса показывают, что опасения компаний в отношении потери определенных типов данных вполне совпадают с тем, что в действительности оказывается в руках третьих лиц в результате инцидента ИБ. Это говорит о том, что компании сравнительно адекватно оценивают риски информационной безопасности, а тот факт, что доля похищений некоторых типов информации снизилась по сравнению с прошлым годом – о том, что меры, которые компании принимают для защиты своих данных, достаточно эффективны. Однако этих мер все еще недостаточно для того, чтобы значительно снизить количество киберинцидентов или вовсе исключить их.

ВИРТУАЛИЗАЦИЯ



В российских компаниях виртуализация даже более популярна, чем в среднем в мире. По данным опроса, 56% российских компаний уже используют виртуализацию серверов, и еще 8% планируют внедрение технологии в течение ближайшего года. Виртуальные рабочие станции уже внедрили в четверти компаний, и 14% планируют сделать это в течение года. Самыми популярными приложениями, с которыми компании предпочитают работать в виртуальной среде, являются базы данных (Oracle, Microsoft SQL Server и др.) – их отметили 48% опрошенных. Еще 37% используют виртуализацию для приложений по управлению финансовой деятельностью и для бухгалтерских программ, и 36% – для почты и коммуникационных приложений.

При этом лишь 18% российских компаний приняли все меры по обеспечению информационной безопасности виртуальной инфраструктуры, в то время как в 65% организаций защита внедрена частично.

Любопытно, что из тех компаний, которые находятся на стадии внедрения защитных систем, 39% выбирают традиционные решения, разработанные для обычной физической инфраструктуры и устанавливаемые на каждую виртуальную машину (решения на базе агента). Из них 30% объясняют свой выбор тем, что такое решение для защиты от вредоносного ПО обеспечивает более высокий уровень безопасности и производительности по сравнению с узкоспециализированными решениями для защиты виртуальных сред.

Специализированные решения для защиты виртуальной среды (большинство функций сканирования/обеспечения безопасности в них реализованы на уровне гипервизора, без установки агента на каждую виртуальную машину) используют 29% опрошенных компаний. И еще 23% используют решения на базе легкого агента.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СЕГМЕНТЕ СРЕДНЕГО И МАЛОГО БИЗНЕСА

В случае успешной атаки небольшие предприятия теряют в среднем 780 тысяч рублей за счет вынужденного простоя, упущенной прибыли и расходов на дополнительные услуги специалистов. Пятерку самых распространенных угроз, которым подвергался СМБ-сегмент в этом году, составляют: вирусные атаки и вредоносные программы (75%), уязвимости в ПО (44%), случайные утечки в силу человеческого фактора (28%) и фишинг (28%), а также сетевые атаки (22%).

Значительный финансовый ущерб от одного инцидента кибербезопасности объясняется, в частности, тем, что в 42% компаний злоумышленники получили доступ к внутренней рабочей информации, в том числе к деталям бизнес-процессов, сообщениям электронной почты и др. Персональные данные клиентов были похищены у 34% предприятий. В общей сложности из-за внешних или внутренних угроз теряли данные две трети СМБ-компаний.

Также в результате опроса выяснилось, что компании малого и среднего бизнеса недооценивают мобильные угрозы: две трети организаций не принимают меры для защиты смартфонов сотрудников. При этом российские СМБ-организации активно осваивают современные технологии – четверть предприятий СМБ-сегмента интегрировала мобильные устройства в собственную инфраструктуру. Однако лишь 32% респондентов сообщили о внедрении продуктов для обеспечения безопасности смартфонов и планшетов. Еще 22% планируют внедрение защиты для мобильных устройств в ближайшем году, а остальные сейчас не видят в этом необходимости, несмотря на рост числа мобильных угроз и связанных со смартфонами и планшетами инцидентов безопасности. За исследуемый период 15% компаний столкнулись с кражей мобильных устройств, при этом в каждом четвертом случае была утрачена критически важная информация. Еще в 17% случаев к утечке важных для бизнеса данных привела потеря мобильных устройств сотрудниками.

ЗАКЛЮЧЕНИЕ: ВАЖНОСТЬ ВЫБОРА ПОДХОДЯЩЕЙ ЗАЩИТЫ

Главный вывод, который можно сделать на основании результатов опроса, заключается в том, что несмотря на более прагматичный и точечный подход российских компаний к обеспечению информационной безопасности своей IT-инфраструктуры, количество успешных атак на бизнес продолжает расти.

В целом компании стали более глубоко вникать в суть существующих рисков информационной безопасности и адресно защищаться от конкретных угроз. Об этом свидетельствует, например, возросший приоритет защиты данных от таргетированных атак. Однако не стоит забывать о том, что спрос на нелегальные услуги по осуществлению подобных атак неуклонно растет, а значит, защититься от них будет все сложнее. Усугубляет ситуацию и тот факт, что с точки зрения сценария и используемых средств, целевые атаки уникальны и готовятся с учетом специфических особенностей компании-жертвы.

Еще одна важная тенденция заключается в том, что хотя с некоторыми угрозами компании стали сталкиваться значительно реже, чем в прошлом году, в целом доля организаций, имевших дело с какой-либо киберугрозой хотя бы один раз за истекшие 12 месяцев, возросла.

Современный рынок средств информационной безопасности достаточно развит, чтобы предоставить клиентам исчерпывающий выбор решений и сервисов для защиты практически любого сегмента IT-инфраструктуры. Проблемой в этой ситуации становится выбор правильной комбинации компонентов защиты, выстраивание бизнес-процессов и политик ИБ, а также создание эффективной системы управления безопасностью компании.

В России для небольших компаний проблему составляет остаточный принцип, которым часто руководствуются владельцы малого бизнеса в отношении обеспечения информационной безопасности своих предприятий. Недостаточное внимание к вопросам ИБ приводит к росту расходов: средняя цена, которую платит СМБ-компания за одну успешную атаку, за год выросла более чем на 100 тысяч рублей.

Опираясь на результаты опроса, специалисты «Лаборатории Касперского» подготовили ряд рекомендаций, которые помогут компаниям существенно повысить уровень своей защищенности от киберугроз.

ОДНОГО ЛИШЬ АНТИВИРУСА НЕДОСТАТОЧНО

Едва ли этот тезис можно назвать новым, однако в последнее время в связи с ростом количества целевых атак, направленных на похищение критически важных конфиденциальных данных и денег, он актуален как никогда. Антивирусное ПО для защиты рабочих станций – необходимая мера, однако не менее важно применять ПО для мониторинга и своевременного устранения уязвимостей, защиту от DDoS- и целевых атак, средства для обеспечения безопасности корпоративных мобильных устройств и пр. Другими словами, компаниям следует применять комплексный подход к обеспечению информационной безопасности.

ВСЕ ЭЛЕМЕНТЫ IT-ИНФРАСТРУКТУРЫ НУЖДАЮТСЯ В ЗАЩИТЕ

До сих пор для многих компаний представление об IT-инфраструктуре ограничивается офисными компьютерами, серверами и сетевым оборудованием, поддерживающим каждодневные бизнес-операции предприятия. Как правило, промышленное оборудование, торговые терминалы, системы жизнеобеспечения и контроля физической безопасности не входят в перечень объектов, нуждающихся в защите от кибератак. При этом нередко подобные системы работают на той же аппаратно-программной платформе, что и офис, а кроме того, часто они соединены между собой. Подобная ситуация делает компанию более уязвимой для атак злоумышленников.

Следует отдельно отметить возросшее количество смартфонов и планшетов, которые сотрудники используют как в личных целях, так и для работы – их защите по-прежнему не уделяется достаточное внимание.

Российским компаниям следует сфокусироваться на применении специальных политик безопасности и соответствующей настройке оборудования, а также внедрении защитных решений, созданных специально для отдельных элементов IT-инфраструктуры.

ЗАЩИТА НЕ БУДЕТ ЭФФЕКТИВНОЙ БЕЗ ОБУЧЕНИЯ СОТРУДНИКОВ И ВНЕДРЕНИЯ ПОЛИТИК БЕЗОПАСНОСТИ

Как показали результаты опроса, значительная часть инцидентов информационной безопасности, приводивших к утечке конфиденциальных данных, происходила по вине сотрудников компании, случайно или намеренно провоцировавших потерю ценной информации. Для того чтобы избежать случайных утечек, компаниям следует повышать уровень образованности сотрудников в области информационной безопасности. Особенно это касается обращения с корпоративной информацией, хранящейся на мобильных устройствах. Политики безопасности, определяющие ответственность сотрудника за распространение конфиденциальной информации, – еще одна мера, которая может существенно повысить уровень защищенности корпоративных данных.

www.kaspersky.ru/business

KASPERSKY lab