Кибербезопасность на новом витке: готовимся противостоять киберугрозам

20-е международное исследование EY в области информационной безопасности за 2017-2018 годы

EY

Совершенствуя бизнес, улучшаем мир

Выводы международного исследования

Международное исследование EY в области информационной безопасности посвящено главным сложностям в сфере кибербезопасности, с которыми сегодня сталкиваются компании во всем мире. В основу исследования были положены ответы 1200 респондентов из разных стран, представляющих организации из более чем 20 секторов экономики. Приведенные ниже выводы базируются не только на результатах исследования, но и на нашем обширном опыте работы с клиентами во всем мире в области совершенствования их программ кибербезопасности.

Результаты исследования показывают, что компании по-прежнему ставят во главу угла вопросы кибербезопасности и достигают существенного прогресса в решении задач, связанных с обнаружением и устранением слабых звеньев в своей системе защиты, однако многообразие и сложность угроз вызывают серьезную обеспокоенность у организаций как никогда ранее.

Потеря киберустойчивости в условиях растущей конвергенции

В наступившую эпоху господства Интернета каждая организация становится цифровой по определению и так или иначе использует в своей деятельности онлайн-технологии и процессы, а также переходит на новые принципы организации труда. Более того, в условиях растущей конвергенции, чему способствует бурное развитие Интернета вещей (IoT), цифровой ландшафт становится бескрайним, и каждый актив, которым владеет или пользуется организация, представляет лишь звено в бесконечной цепи взаимосвязанных элементов. Сегодня компаниям сложнее чем когда-либо четко обозначить границы цифровой среды, в которой они работают.

Подобные условия создают благодатную почву для хакерских атак. Объектом внимания злоумышленников являются как крупные, так и небольшие компании государственного и частного сектора, причем атаки могут быть как массовыми, так и нацеленными на конкретную организацию. Хакеры научились хорошо маскироваться, и чтобы эффективно противостоять их атакам, необходимо иметь на вооружении такие средства киберзащиты, которые способны распознать угрозу, даже когда она не заметна на общем фоне.

В сложившейся ситуации организациям необходимо оценить свою устойчивость к следующим видам угроз:

Обычные атаки
К этой категории относятся атаки со стороны «простых» хакеров, которые, зная об уязвимостях в той или иной системе защиты, пытаются взломать её при помощи бесплатных хакерских утилит. Для успешного проведения подобного рода атак не требуется особый опыт и умения.

Сложные атаки
Такие атаки зачастую выполняют умелые хакеры, во-оруженные передовыми техническими средствами и методиками и знающие о критических точках уязвимости в системе защиты организации, о которых ей самой не всегда известно (т.н. уязвимости «нулевого дня»).

Новые атаки
Это принципиально новый вид атак, которые проводятся с прицелом на уязвимости в системах и обусловлены появлением новых технологий. Как правило, на подобные атаки идут наиболее технически подкованные злоумышленники, которые заранее проводят тщательную подготовительную работу, чтобы иметь возможность определить слабые звенья в системе защиты и воспользоваться ими.

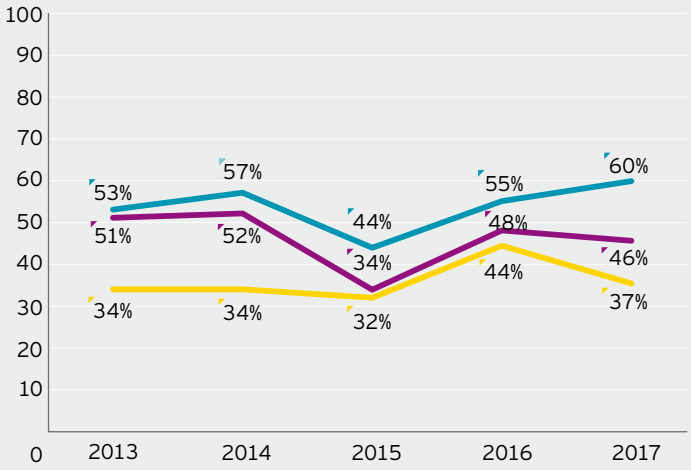
Сравнение ключевых выводов и данных по всему миру и России

Весь мир	Россия	
87%	71%	респондентов отмечают необходимость увеличения бюджета на кибербезопасность до 50%.
77%	77%	респондентов полагают, что неосмотрительные сотрудники являются наиболее вероятным источником киберугрозы.
12%	30%	респондентов считают, что с большой долей вероятности смогут распознать изощренную кибератаку.
63%	31%	организаций по-прежнему возлагают обязанности по подготовке отчетности о кибербезопасности на ИТ-службу.
48%	42%	не создали центров обеспечения информационной безопасности, несмотря на все более широкое распространение подобной практики.
17%	49%	респондентов заявляют, что высшее руководство их организаций обладает достаточными знаниями в области информационной безопасности, чтобы осуществлять эффективный надзор за киберрисками.
57%	69%	либо совсем не имеют специальной программы в области сбора и анализа информации о киберугрозах, либо ограничиваются неформальными мероприятиями в этой сфере.
89%	98%	респондентов признают, что их служба кибербезопасности не в полной мере соответствует потребностям организации.

Угрозы и уязвимости, которые играют решающую роль в увеличении рисков организации. Данные опроса за 2013-2017 годы.

Уязвимости

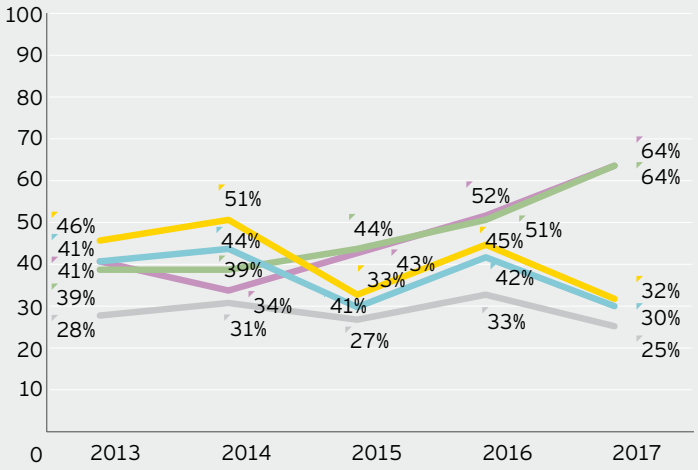
% респондентов, которые поставили рассматриваемую уязвимость на первое или второе место по актуальности для бизнеса



- Неосмотрительность и неосведомленность сотрудников
- Устаревшие средства контроля или архитектура безопасности
- Несанкционированный доступ

Угрозы

% респондентов, которые поставили рассматриваемую угрозу на первое или второе место по актуальности для бизнеса



- Вредоносное ПО
- Фишинг
- Кибератаки с целью кражи финансовой информации
- Кибератаки с целью кражи интеллектуальной собственности или данных
- Внутренние атаки

Сравнивая ключевые выводы и результаты исследования по всему миру и России, мы отмечаем существенные отличия по ряду направлений, особенно в части способности идентификации изощренных атак (весь мир – 12%; Россия – 30%). Мы полагаем, что в России слишком высока степень доверия к техническим средствам защиты информации. Однако наш обширный опыт реализации проектов указывает на недостаток функциональной и технической обеспеченности информационной безопасности. Дополнительно хотим отметить, что использование только технических решений и экспертизы специалистов ИБ в отрыве от выстраивания процессной модели обеспечения кибербезопасности в организации не гарантирует должной защиты от новых атак, в ходе которых злоумышленники используют продвинутые механизмы сокрытия и удержания своего продолжительного присутствия в корпоративной сети.

Эффективное управление информационной безопасностью требует также повышения уровня зрелости всех ее процессов, повышения уровня компетенций персонала служб ИБ, ИТ, а также пользователей систем и руководства организаций.

Несмотря на то, что в ряде случаев данные по России выглядят более привлекательными, при детальном рассмотрении отмечается общее отставание по уровню зрелости процессов управления кибербезопасностью и их интеграции с бизнес-процессами.

Кибербезопасность на новом витке: выстраивание защиты, отвечающей требованиям сегодняшнего дня...

Не исключено, что в скором времени на многие организации обрушится целая волна хакерских атак – от самых простых до наиболее изощренных. Подобным атакам можно и нужно уметь давать отпор. Необходимо принимать решительные ответные меры по всем фронтам, начиная с противостояния наиболее распространенным атакам и заканчивая применением более «тонких» подходов для противодействия продвинутым и принципиально новым видам атак. Поскольку полностью защититься от атак невозможно, и какая-нибудь из них непременно пробьет брешь в защите, следует прежде всего сосредоточиться на том, как оперативно выявить такую атаку и эффективно справиться с ее последствиями.

- Защититься от обычных атак означает уметь держать свою «границу» на замке. Ключевыми составляющими устойчивости организации к подобным видам атак являются такие традиционные средства, как антивирусные программы, системы обнаружения и предотвращения вторжений (IDS и IPS), регулярное обновление программного обеспечения, а также технологии шифрования, обеспечивающие целостность данных даже в том случае, если злоумышленникам удастся получить к ним доступ. Важным элементом выстраивания надежной системы защиты также является информирование сотрудников на всех уровнях организационной иерархии с целью формирования ответственного отношения к вопросам кибербезопасности, включая обеспечение неукоснительного соблюдения требований парольной политики.
- Защититься от сложных атак означает признать, что несанкционированное проникновение может произойти в любой момент, и быть способным как можно раньше его обнаружить. Отправной точкой в организации эффективного выявления киберугроз является создание центра обеспечения информационной безопасности (SOC), который должен стать центральным штабом, координирующим всю работу по этому направлению. Сегодня все чаще можно наблюдать трансформацию функций SOC от пассивной защиты к активной обороне – тщательно спланированной и непрерывной кампании, нацеленной на выявление и нейтрализацию скрытых злоумышленников и борьбу с вероятными угрозами безопасности для наиболее важных активов организации.
- Защититься от новых атак означает признать, что в ряде случаев происхождение угроз будет неизвестным. Несмотря на всю неопределенность, наиболее иннова-

ционно продвинутые организации могут постараться обрисовать для себя контур будущих угроз и выработать такой подход, который позволит принять оперативные меры реагирования в нужный момент. Организации, обладающие надежной системой корпоративного управления, могут разработать системы и процессы, способные эффективно реагировать на неожиданные риски и появляющиеся угрозы, взяв на вооружение принципы «проектируемой безопасности».

Разработка программы и плана действий на случай нарушения информационной безопасности (Cyber resilience)

Сегодня важно осознать, что рано или поздно та или иная атака злоумышленников увенчается успехом. Предварительная подготовка к таким атакам вместе с наличием плана действий на случай нарушения информационной безопасности (cyber breach response plan, CBRP), который автоматически приводится в исполнение при обнаружении кибернарушений, являются наилучшим средством для сведения к минимуму их последствий. Стоит отметить, однако, что подобную программу нарушения информационной безопасности необходимо реализовывать в масштабах всей организации. Руководителем такой программы должен быть специалист, обладающий надлежащим опытом и знаниями в области операционного и стратегического реагирования.

Контактная информация

Николай Самодаев

Партнер, руководитель направления по предоставлению услуг в области бизнес-рисков, управления ИТ и кибербезопасностью в СНГ
Тел.: +7 (405) 755 9869
Nikolay.Samodaev@ru.ey.com

EY

Assurance | Tax | Transactions | Advisory

Краткая информация о компании EY

EY является международным лидером в области аудита, налогообложения, сопровождения сделок и консультирования. Наши знания и качество услуг помогают укреплять доверие общественности к рынкам капитала и экономике в разных странах мира. Мы формируем выдающихся лидеров, под руководством которых наш коллектив всегда выполняет взятые на себя обязательства. Тем самым мы вносим значимый вклад в улучшение деловой среды на благо наших сотрудников, клиентов и общества в целом.

Мы взаимодействуем с компаниями из стран СНГ, помогая им в достижении бизнес-целей. В 20 офисах нашей фирмы (в Москве, Санкт-Петербурге, Новосибирске, Екатеринбурге, Казани, Краснодаре, Ростове-на-Дону, Владивостоке, Тольятти, Южно-Сахалинске, Алматы, Астане, Атырау, Бишкеке, Баку, Киеве, Ташкенте, Тбилиси, Ереване и Минске) работают 4500 специалистов.

Название EY относится к глобальной организации и может относиться к одной или нескольким компаниям, входящим в состав Ernst & Young Global Limited, каждая из которых является отдельным юридическим лицом. Ernst & Young Global Limited – юридическое лицо, созданное в соответствии с законодательством Великобритании, – является компанией, ограниченной гарантиями ее участников, и не оказывает услуг клиентам. Более подробная информация представлена на нашем сайте: ey.com.

Офисы EY

Алматы +7 (727) 258 5960	Краснодар +7 (861) 210 1212
Астана +7 (7172) 58 0400	Минск +375 (17) 240 4242
Атырау +7 (7122) 55 2100	Москва +7 (495) 755 9700
Баку +994 (12) 490 7020	Новосибирск +7 (383) 211 9007
Бишкек +996 (312) 623 096	Ростов-на-Дону +7 (863) 261 8400
Владивосток +7 (423) 265 8383	Санкт-Петербург +7 (812) 703 7800
Екатеринбург +7 (343) 378 4900	Ташкент +998 (71) 140 6482
Ереван +374 (10) 500 790	Тбилиси +995 (32) 215 8811
Казань + 7 (843) 567 3333	Тольятти +7 (8482) 99 9777
Киев +380 (44) 490 3000	Южно-Сахалинск +7 (4242) 49 9090