Review

kaspersky

Умная киберзащита в 2024 году

0+

В России каждая пятая кибератака нацелена на компании из сектора среднего бизнеса, при этом в случае удачной попытки мошенники присваивают себе в среднем пять миллионов рублей. Разобрали несколько инструментов, которые помогут защитить данные и средства компании от киберугроз.

По данным Единого реестра субъектов малого и среднего предпринимательства в Республике Башкортостан за одиннадцать месяцев 2023 года зарегистрированы 135,3 тыс. субъектов малого и среднего предпринимательства, и этот показатель с начала года вырос на 5,9%. Средние и крупные компании зачастую уже на этапе развития внедряют в работу сервисы оцифровки бизнеса и IT-системы. Это нужно для того, чтобы упростить и автоматизировать свои процессы, четко отслеживать рост компании и грамотно взаимодействовать с государственными структурами. Но, несмотря на выгодные стороны оцифровки бизнеса, возникает и угроза кибератак.

Цифровизация процветает и в государственных структурах. Так, по итогам прошлого года Башкирия вошла в топ-10 рейтинга цифровой трансформации регионов и заняла восьмое место. Республика достигла «цифровой зрелости» в сфере здравоохранения, образования, городского хозяйства и строительства, общественного транспорта на 90,33%. Рост цифровизации также провоцирует кибермошенников на более изощренные методы для получения незаконной выгоды.

КОМПАНИИ ПОД УГРОЗОЙ

В 2023 году было зафиксировано более 130 тыс. атак на представителей среднего и крупного бизнеса. Таким образом преступники могут украсть конфиденциальные данные компании, подменить платежные документы для перевода средств на свои счета или надолго остановить деятельность компании, зашифровав компьютеры и серверы.

В России каждая пятая атака нацелена на компании из сектора среднего бизнеса. При этом при удачной попытке мошенникам удается присвоить себе в среднем пять миллионов рублей.

На ресурсе cybermap.kaspersky.com Россия уже третий год отмечена как самая атакуемая в киберпространстве страна. В 2023 году решения «Лаборатории Касперского» обнаруживали в среднем 411 тыс. новых вредоносных файлов ежедневно. Всего с января по декабрь 2023 года решения компании выявили почти 170 млн вредоносных файлов.

Об активности злоумышленников можно судить и по трендам теневого сегмента интернета. В 2023 году специалисты компании наблюдали значительный рост числа объявлений о продаже стилеров или, проще говоря, вредоносных программ и программ-вымогателей на теневых форумах. «Лаборатория Касперского» выявила всплеск сообщений в блогах групп, реализующих атаки программ-вымогателей, где организаторы пишут об успешных взломах публично, чтобы шантажировать компании, и даже иногда выкладывают украденные данные.

Команда Kaspersky Digital Footprint Intelligence в 2022 году ежемесячно обнаруживала в среднем около 386 таких постов, а в 2023 году — уже 476. Риск утечки личных и корпоративных учетных данных стал еще выше. В даркнете увеличилось количество сообщений, относящихся к стилерам — программам для кражи конфиденциальной информации, такой как учетные данные для входа в систему, финансовые реквизиты и личные данные. Например, ежемесячное количество объявлений о продаже лог-файлов Redline, популярного семейства стилеров, выросло в среднем с 370 в 2022 году до 1,2 тыс. в 2023 году. В целом объем публикаций на подпольных форумах со свободным распространением лог-файлов вредоносных программ, содержащих скомпрометированные данные пользователей, вырос в прошлом году, по сравнению с 2022 годом, почти на 30%.

ТРЕНД НА КИБЕРАТАКИ

Чаще всего при покушении на крупный бизнес преступники используют новые технологии для реализации «классических» техник атак, например большие языковые модели для подготовки вредоносных почтовых рассылок. Также в тренде многократная эксплуатация успешной атаки. Это когда у компании требуют выкуп за восстановление данных, затем за их неразглашение, а затем информацию все равно сливают для дополнительного репутационного ущерба. При этом у каждого из этапов схемы могут быть разные выгодополучатели. Также хочется отметить тенденцию переиспользования инструментария, который был когда-то слит — то ли случайно, то ли умышленно — для сокрытия следов истинных злоумышленников.

При этом компании среднего бизнеса все чаще становятся жертвами киберугроз. И если раньше они были направлены, как правило, на крупные корпорации, то за последние полтора-два года мы видим сложные атаки на средний бизнес.

Основной целью атак злоумышленников на компании в большинстве случаев остается финансовая выгода. К примеру, по статистике «Лаборатории Касперского», в четвертом квартале 2022 года среди компаний, обратившихся за восстановлением ценных данных к специалистам по реагированию на киберинциденты, были организации, оказывающие бухгалтерские и клининговые услуги, поставляющие строительные материалы, а также небольшие производства. Но в целом для злоумышленников нет различий с точки зрения отраслей. Есть разная мотивация, цели: финансовая прибыль, кибершпионаж, хактивизм и так далее.

Важно отметить, что небольшие организации, если они являются поставщиками IT-решений для корпораций, используются злоумышленниками как точка входа в крупные корпорации — их могут использовать для проникновения в инфраструктуру крупной компании с помощью так называемых атак на цепочки поставок. Далеко не все кейсы взломов и утечек становятся публичными, потому может создаться обманчивое ощущение, что происходят они не так уж и часто. Но реальная статистика выше как по числу атак, так и по причиненному ущербу. Успешная атака, как правило, приносит ущерб на бóльшую сумму, чем инвестиции в ее предотвращение.

Жертвы несут несколько видов убытков. К примеру, компания не прислушалась к советам специалиста по информационной безопасности, не выстраивала защиту, использовала разрозненные, не интегрированные решения, полностью игнорируя некоторые из угроз, например защиту корпоративной почты. В результате атаки шифровальщика все серверы и компьютеры были выведены из строя, остановилась работа производственных площадок, отгрузки имеющейся готовой продукции. Компания пошла по пути выплаты выкупа. Понесла двойной урон. Отдавая выкуп, поставила себя под регуляторные риски, так как чаще всего злоумышленники требуют выкуп в криптовалюте, которая запрещена на территории России.

Фундамент любой системы информационной безопасности — это защита конечных точек, то есть серверов, корпоративных компьютеров, смартфонов и планшетов. Также сегодня необходима специализированная защита корпоративной почты и вебтрафика. Среднему бизнесу — дополнительно к базовым средствам защиты — рекомендуется использовать решения для работы с инцидентами, созданные специально для предприятий этого сегмента, из линейки Kaspersky Smart. Внедрение таких решений позволит защитить организацию от более сложных киберугроз.

Кроме того, по мнению экспертов компании, стоит инвестировать в тренинги по кибербезопасности для сотрудников — от обычных работников до профильных специалистов. Персонал важно обучать безопасному поведению в Сети, в том числе тренировать навыки работников с помощью имитации фишинговых атак.

В стремительно развивающихся компаниях, где насчитывается уже несколько сотен сотрудников, руководители зачастую создают отдел информационной безопасности. Однако, если рост и масштабирование не прекращаются, у сотрудников отдела, которые отвечают за сохранность цифровых данных, может не хватать времени и инструментов. В такие моменты стоит задуматься, а как еще можно защитить свой бизнес от киберугроз?

ПРИВЫЧНЫЙ СЦЕНАРИЙ

Как обычно защищаются от киберугроз владельцы малого или среднего бизнеса? В первую очередь обычно это установка так называемого антивируса, который выявляет вредоносные программы и предотвращает заражение рабочих систем, позволяет сделать резервные копии в случае утери информации. Такой инструмент, конечно, эффективный, но только не в случае целевой и точечной кибератаки.

Хакер, обладающий нужными знаниями и достаточной мотивацией для того, чтобы получить желаемые данные, очень просто может обойти такое одиночное защитное решение. Он потратил много времени на изучение и анализ информации о компании и точно знает, какую защиту ему обходить и какие для этого найдутся подручные средства. Также стоит помнить, что некоторые хакеры не используют вредоносных программ, чтобы не оставлять за собой следов. В таком случае, если его действия принесут результат и компании будет нанесен ущерб, провести полноценное расследование и выявить его шаги будет достаточно сложно. В результате компания может потерять активы, а после потратит много ресурсов на расследование и устранение последствий.

КАК ЭТОГО ИЗБЕЖАТЬ?

Кроме классической антивирусной программы компаниям стоит подумать о внедрении систем безопасности, которые обеспечат защиту в более сложных случаях: при атаке на серверы, рабочие станции и виртуальные машины, при обнаружении подозрительной активности и не обязательно вредоносной. А еще такие защитные системы смогут быстро проанализировать текущую ситуацию, создать отчет, вовремя отреагировать на инцидент и автоматически провести расследование.

Конечно, все эти действия можно совершить в ручном режиме, а также поручить отделу ИБ прописать сценарии для автоматизации. Но этот способ малоэффективен, поскольку на него уходит очень много времени. А отдел ИБ всегда перегружен текущими задачами вроде установки защитных продуктов и настройки прав доступа. Более того, мониторинг «на коленке» может сбивать команду ИБ, отвлекать ложными срабатываниями. В связи с этим возникает риск не заметить те самые важные события, не изучить досконально информацию об инциденте и не среагировать на него вовремя.

ЭФФЕКТИВНАЯ ЗАЩИТА

Новые технологии создаются для того, чтобы упрощать ручные процессы и оптимизировать работу компаний. Именно поэтому для эффективной информационной безопасности крупные компании давно используют решения SIEM (Security Information and Event Management), которые автоматически собирают данные из всевозможных источников (телеметрия или события в приложениях и на серверах), объединяют их в группы и позволяют в короткий срок проанализировать все действия, связанные с цифровой инфраструктурой компании. Такой подход к событиям и сбору данных помогает специалистам по информационной безопасности проще обнаружить инциденты и быстрее провести расследование, составить отчет и передать данные руководству.

Благодаря «Лаборатории Касперского» подобные решения стали доступны и для среднего бизнеса. Новая система Kaspersky Smart I позволяет компаниям защищать свои данные и экономить финансы. Во-первых, лицензии стоят намного меньше, чем установка «корпоративного» SIEM. Во-вторых, решение от «Лаборатории Касперского» — легкое и не требует дорогого и мощного оборудования, его можно запустить на уже имеющихся серверах. К тому же система имеет множество правил отслеживания и сценариев реагирования, поэтому тратить время на ручную настройку не придется. В-третьих, система высоко автоматизирована и не нуждается в большом количестве сотрудников для ее ежедневного обслуживания.

Согласно статистике компании-разработчика, в первой половине 2023 года решения «Лаборатории Касперского» детектировали в России 95 879 срабатываний вредоносных файлов на устройствах сотрудников компаний малого и среднего бизнеса.

На средний бизнес сейчас приходится каждая пятая кибератака, причем компании среднего размера часто подвергаются не только массовым, но и сложным, таргетированным атакам.

Такая система безопасности идеально подойдет для средних компаний из финансового сектора, сферы страхования, ритейла, здравоохранения, агропромышленного комплекса, государственных и других организаций. При этом она не требует покупки дорогостоящего оборудования и может быть развернута как локально, так и в виртуальной среде.

Поскольку многие российские компании и так используют решения «Лаборатории Касперского», им будет очень просто объединить эти системы, чтобы в SIEM поступали дополнительные данные из защитного решения на компьютерах, а в обратную сторону шли команды, например, на автоматическое устранение уязвимостей или других проблем информационной безопасности. Еще одним веским плюсом является то, что решение входит в Единый реестр отечественного ПО Минцифры Российской Федерации и закрывает существенную часть имеющихся регуляторных требований по ИБ.

ЕСЛИ УГРОЗА СЛИШКОМ ВЫСОКА

Решения SIEM помогут собрать максимальное количество данных об инцидентах, но для эффективного сбора самой ценной и важной информации (о событиях в конечных точках, то есть в рабочих компьютерах и серверах) применяется другое защитное решение — EDR (Endpoint Detection and Response). Эта система незаменима для анализа подозрительных, но не обязательно вредоносных событий.

При работе данной системы специалист по информационной безопасности может запросить дополнительную информацию о любой активности на сервере, собрать ее и в случае обнаружения угрозы заблокировать сетевую активность на зараженном компьютере и сбросить пароли до ужесточения политики безопасности для компьютера. Таким образом, EDR служит «страховочной сеткой», которая позволяет обнаружить и пресечь опасную активность, возможно, не замеченную базовым защитным решением. Но стоит отметить, что такая система не заменяет антивирус (базовую защиту), но может очень эффективно работать в тандеме с ним, предотвращая разные виды кибератак.

Как раз для таких компаний, которые хотят еще более надежно защитить свои данные от злоумышленников, подойдет Kaspersky SMART II — решение, объединяющее SIEM и EDR. Это комплексное решение, которое позволяет обнаруживать и останавливать сложные целевые атаки, вести расследования инцидентов и оперативно принимать решения по ним. Такая система работает с каждым подключенным компьютером и собирает с них расширенный набор данных, реагируя даже на продвинутые киберугрозы. Эта комбинация решений дает полную видимость в сети для анализа первопричин и расследования инцидентов.

Приобрести Kaspersky Smart или записаться на его демонстрацию можно, заполнив форму на официальном сайте или обратившись к партнёрам «Лаборатории Касперского» — они работают по всей России.

«Лаборатория Касперского» — международная компания, работающая в сфере информационной безопасности и цифровой приватности с 1997 года. Технологии «Лаборатории Касперского» защищают более 400 миллионов пользователей и 220 тысяч корпоративных клиентов во всем мире. Компания также создает кибериммунные решения, которые базируются на микроядерной операционной системе KasperskyOS и обеспечивают безопасность по умолчанию.