Как российские компании защищаются от целевых атак

Positive Technologies

ptsecurity.com

Описание исследования

По данным исследования Positive Technologies, треть специалистов по ИБ сообщили, что их компании когда-либо подвергались целевой атаке, в большинстве случаев — с серьезными последствиями. В каждом пятом случае организации защищаются с помощью систем класса NTA и Sandbox. На российском рынке есть тенденция к расширению арсенала средств безопасности и выявлению APT-атак с помощью комплексных решений.

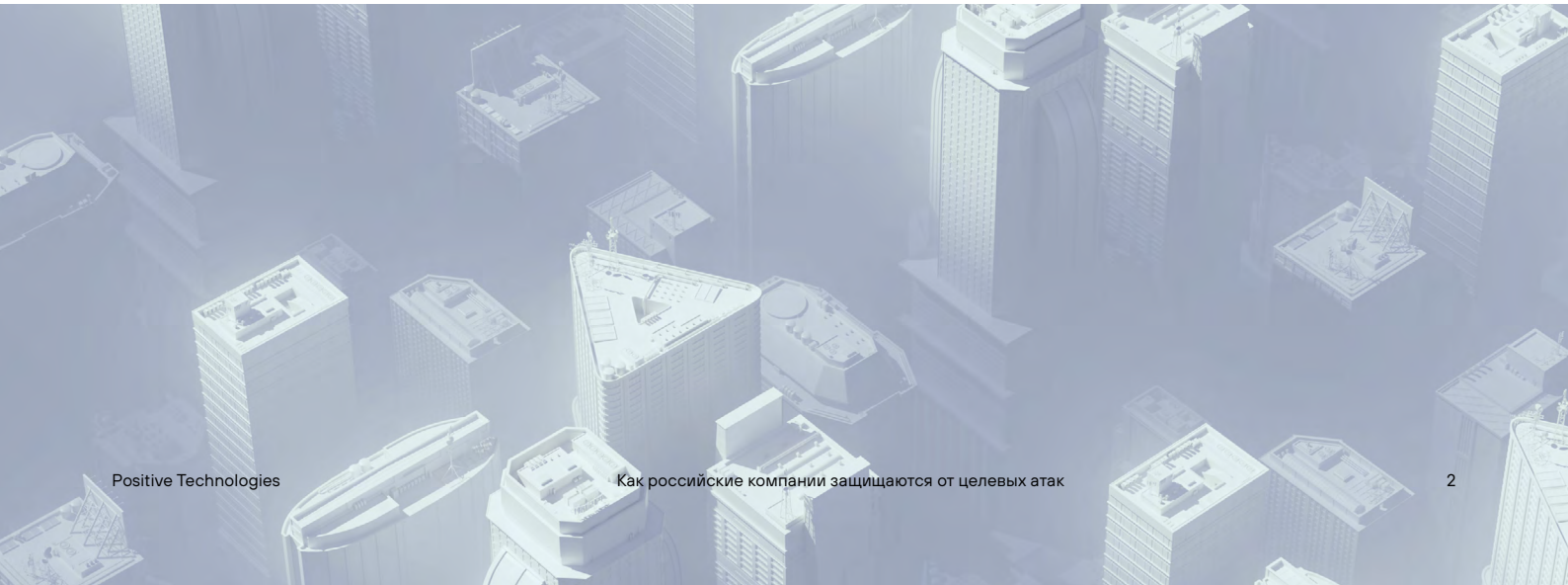
Подробнее о том, насколько надежно российские компании защищены от целевых атак и какие способы защиты используют, читайте в отчете.

На прочтение:
10 минут

Целевой считается кибератака, направленная на конкретную компанию, отрасль экономики или ограниченный круг частных лиц. Прежде чем атаковать, злоумышленники, как правило, проводят предварительную разведку и собирают информацию о выбранной жертве.

По данным исследования Positive Technologies, треть компаний когда-либо подвергалась целевой атаке, в большинстве случаев — с серьезными последствиями. Насколько надежно организации защищены от таких угроз и какие тенденции в использовании средств защиты можно отметить, расскажем далее.

Мы провели анонимный опрос представителей разных отраслей: финансовой, промышленной, государственного сектора, ТЭК, образования, телекоммуникаций, здравоохранения, СМИ и IT. Чаще всего страдают финансовые организации: 44% респондентов сферы сообщили о целевых атаках, на втором месте ТЭК — 33%, а замыкают тройку государственные компании — 29%.



Чем опасны целевые атаки

В качестве основной цели, которую преследуют злоумышленники, большинство опрошенных отмечает кражу ценной информации (рис. 1). Однако в сфере образования больше половины представителей (63%) считает, что таким образом атакующие стремятся нанести удар по репутации компании.

С какой целью, на ваш взгляд, вашу компанию может атаковать хакерская группировка?

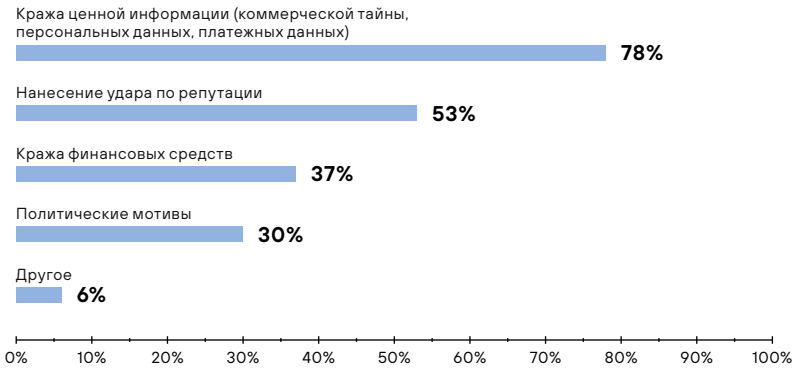


Рисунок 1.

Целевые атаки наносят ощутимый урон и могут напрямую повлиять на работу организации, в том числе на ее финансовые результаты. Респонденты отмечают, что в результате подобных атак они чаще всего сталкивались с такими последствиями, как простой инфраструктуры, нарушение бизнес-процессов и уничтожение или изменение данных (рис. 2).

В 16% случаев компании платили выкуп злоумышленникам. Мы рекомендуем не идти на поводу у атакующих и обращаться к специалистам для устранения последствий атаки. Нет гарантий, что злоумышленники восстановят работоспособность инфраструктуры, прекратят шантаж и не потребуют дополнительных денег.

С какими последствиями кибератак сталкивалась компания?

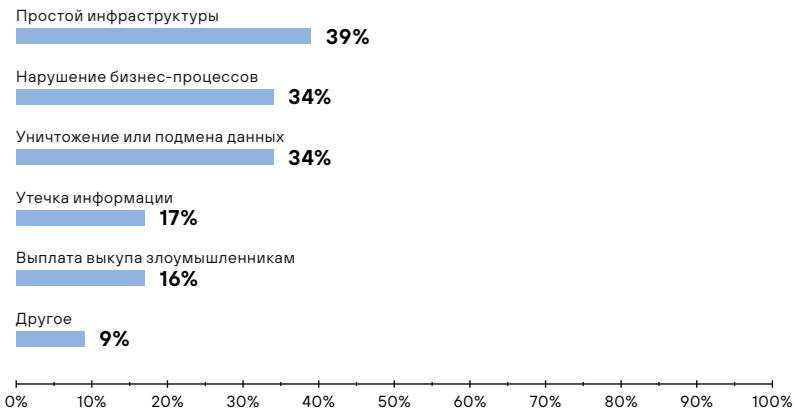


Рисунок 2.

Защита от кибератак

В ответах на вопросы об используемых средствах защиты от целевых атак есть печальная тенденция: в основном в арсенале компаний есть только базовые инструменты безопасности, которые не заточены под выявление сложных угроз. До сих пор не во всех компаниях установлены даже антивирусные средства защиты.

Классы решений, которые действительно способны обнаружить злоумышленника в сети, использует только каждая четвертая компания: Sandbox — 28% опрошенных, решения класса NTA — 27% (рис. 3).

Какие системы информационной безопасности используются в компании для выявления кибератак?

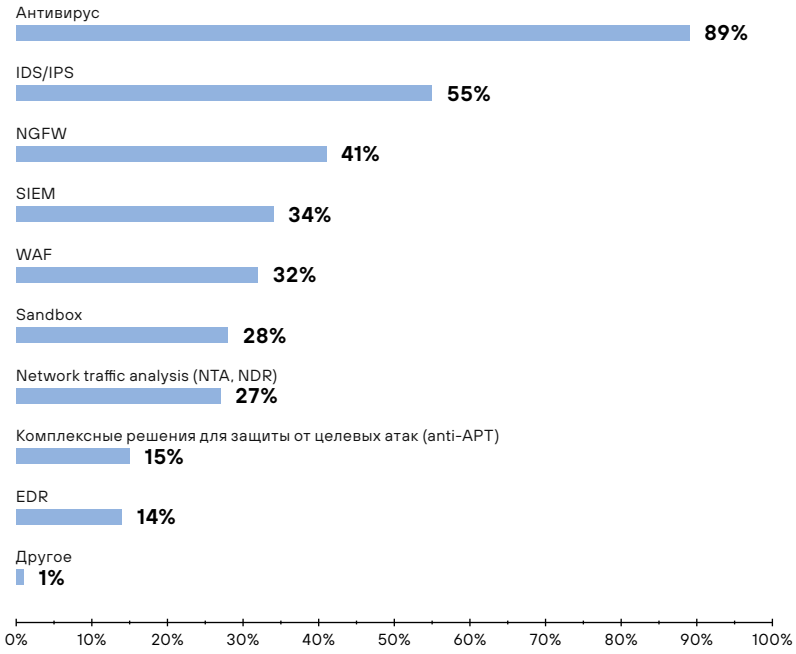


Рисунок 3.

Почему недостаточно базовых средств защиты?

В инфраструктуре злоумышленники способны скрыть следы присутствия, но стереть их в трафике невозможно. Эту особенность использует система глубокого анализа трафика (NTA) PT Network Attack Discovery. Она позволяет выявлять атаки на периметре и внутри сети, а также замечает любую сетевую активность.

Атаки с использованием ВПО по-прежнему занимают первое место в арсенале киберпреступников: их доля во II квартале 2021 года составила 73%. Одна из причин успеха таких атак — злоумышленники совершенствуют вредоносное ПО так, чтобы его не смогли обнаружить базовые средства защиты: антивирусы, межсетевые экраны, IPS, почтовые и веб-шлюзы. Поэтому есть отдельный класс решений для выявления вредоносов — песочница. Она запускает файл в изолированной виртуальной среде, анализирует его действия в системе и выносит вердикт, безопасен он или нет.

Благодаря гибкой настройке виртуальных сред в соответствии с реальными рабочими станциями компании, PT Sandbox поможет эффективно выявлять ВПО, которое используется в целевых атаках.

Мы спросили у респондентов, как их компании планируют защищаться в ближайшие 1–3 года. Хорошие новости: каждая пятая организация намерена начать использовать NTA-систему и комплексные решения для защиты от целевых атак (рис. 4). Это значит, что их способность обезопасить себя от таких угроз вырастет.

Отраслевая специфика: в планах 39% специалистов из IT-компаний — приобрести песочницу для выявления сложных угроз. Представители промышленности планируют закупать SIEM (40%), NTA (36%), Sandbox (36%). В финансовой отрасли, помимо комплексных решений для защиты от целевых атак (40%), 27% организаций будут усиливать защиту с помощью EDR и NGFW.

Какие системы информационной безопасности вы планируете начать использовать для выявления кибератак в ближайшие 1–3 года?

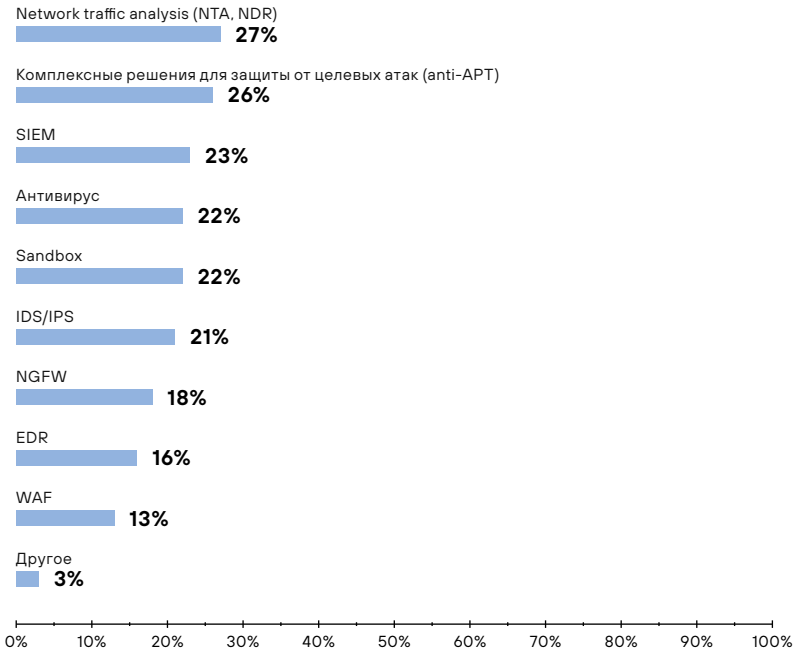


Рисунок 4.

MITRE ATT&CK — это база знаний, разработанная и поддерживаемая корпорацией MITRE на основе анализа реальных APT-атак. Это структурированный в виде наглядной таблицы список тактик, для каждой из которых указаны возможные техники.

В завершение опроса мы узнали у респондентов, знают ли они о матрице MITRE и используют ли ее для создания стратегии защиты от целевых атак.

С помощью нее специалисты по ИБ могут отслеживать информацию об актуальных угрозах и с учетом этих данных строить эффективную систему безопасности. Знание того, как действуют реальные APT-группировки, помогает строить гипотезы для проактивного поиска угроз в рамках threat hunting (mitre.ptsecurity.com).

С какой целью, на ваш взгляд, вашу компанию может атаковать хакерская группировка?

Радует, что в общей сложности 67% опрошенных специалистов знают о матрице MITRE: они либо уже пользуются ее данными, либо планируют (рис. 5).

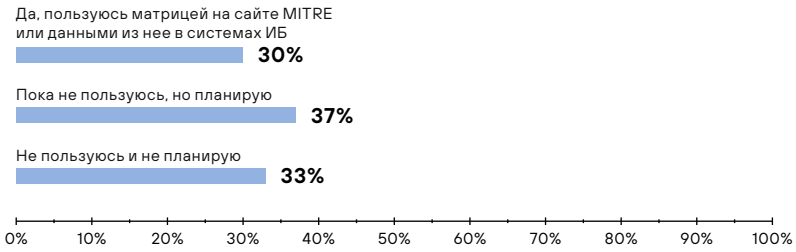


Рисунок 5.

Вывод

В каждой отрасли были компании, которые подверглись целевым атакам. При этом большинство организаций практически не защищены от таких угроз: в основном используют базовые средства защиты, у некоторых нет даже антивирусов. Лишь 10% респондентов имеют специализированные комплексные решения.

Есть и позитивные тенденции. Компании понимают необходимость повышения уровня безопасности, планируют расширять арсенал средств защиты, включать в него специализированные комплексные решения для выявления целевых атак. Растет интерес и к MITRE ATT&CK. Раз есть потребность в подобных инструментах, целесообразно было бы адаптировать матрицу под запросы российского рынка.

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays