Актуальные киберугрозы на Ближнем Востоке

2022–2023

Positive Technologies

ptsecurity.com

Содержание

Основные проблемы кибербезопасности в Ближневосточном регионе

Обстановка в киберпространстве Ближнего Востока — одна из наиболее напряженных во всем мире. Сочетание процветающей экономики и высоких темпов цифровизации привлекают внимание злоумышленников. Убытки ближневосточных стран от кибератак с каждым годом становятся больше: по данным IBM за 2020 год, ущерб от кибератак на организации в Саудовской Аравии и Объединенных Арабских Эмиратах в среднем составил 6,53 млн долларов, что больше среднего показателя по всему миру на 69%. Согласно прогнозу Research and Markets, ожидается, что размер рынка кибербезопасности на Ближнем Востоке увеличится почти до 30 млрд долларов к 2025 году при среднегодовом темпе роста 14%.

Помимо растущей киберпреступности, можно выделить ряд проблем информационной безопасности, которые могут в значительной степени влиять на достижение операционных и стратегических целей организаций и на уровень защищенности целых стран.

Кибератаки на критически важную инфраструктуру

Ближний Восток является одним из наиболее важных регионов в мире с точки зрения добычи нефти и газа (например, в Саудовской Аравии в 2021 году добывалось почти 11 млн баррелей нефти в сутки), а также транспортировки добытых ресурсов. Это делает ближневосточные страны особенно уязвимыми для кибератак на ключевые объекты инфраструктуры, такие как нефтяные и газовые месторождения, электростанции, порты, аэропорты: аналитики «Лаборатории Касперского» сообщили, что в 2022 году Ближний Восток попал в пятерку регионов мира с наибольшим процентом блокирования вредоносного ПО в автоматизированных системах управления (АСУ).

Кибервойны, кибершпионаж и хактивизм

Геополитическая напряженность региона приводит к постоянной активности хорошо подготовленных групп злоумышленников (advanced persistent threats, APT), которые совершают целевые кибератаки и ведут кибершпионаж. Кроме того, в ближневосточных странах актуальна угроза хактивистов — злоумышленников, кибератаки которых направлены не на получение финансовой выгоды или сбор данных, а на привлечение внимания общественности к различным социальным или политическим проблемам (например, путем массированных DDoS-атак или дефейса сайтов).

Сводная статистика по кибератакам на Ближнем Востоке

Рисунок 1. Количество успешных кибератак в Ближневосточном регионе (по кварталам)

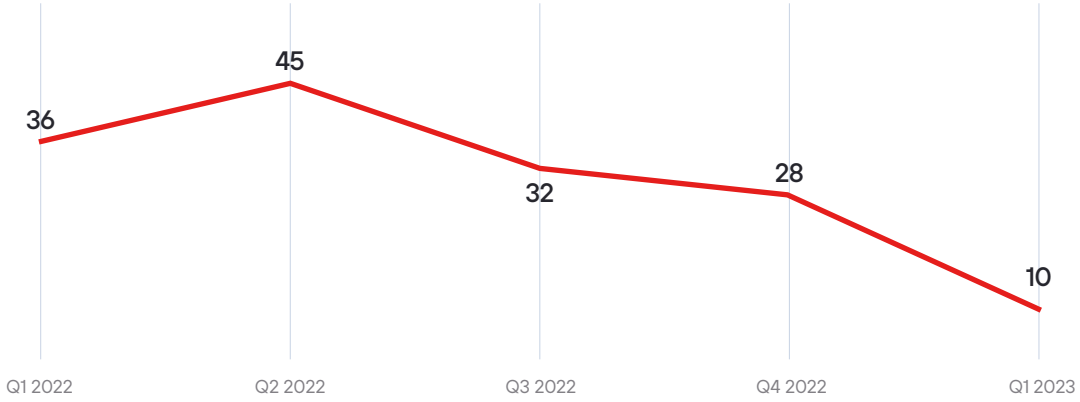
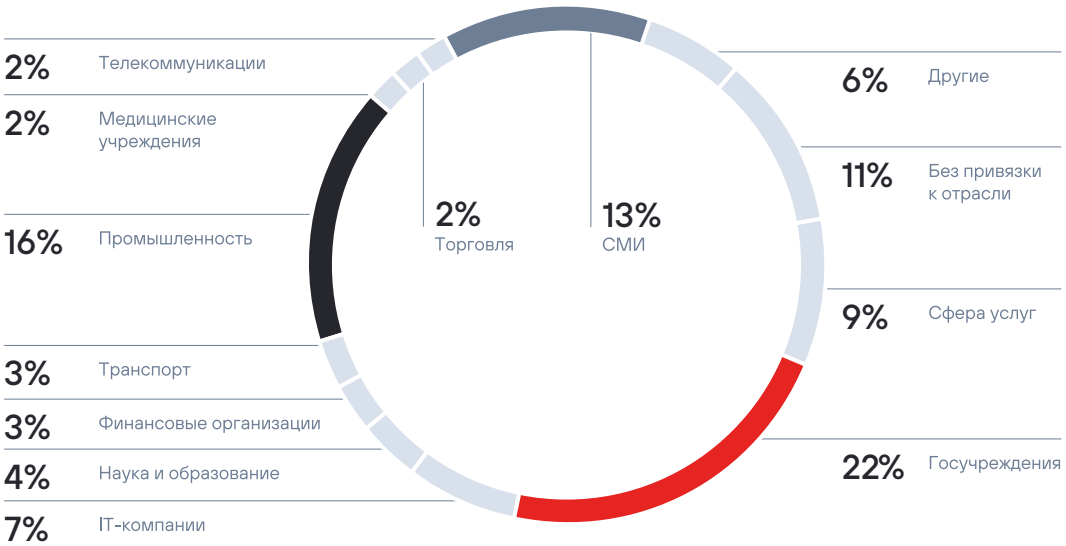


Рисунок 2. Категории жертв среди организаций

83%
успешных атак имели целенаправленный характер

20%
атак были направлены на частных лиц



Государственные учреждения

В странах Ближнего Востока государственные учреждения являются наиболее привлекательными целями для киберпреступников: на их долю пришлось 22% от общего числа атак на организации. Основными последствиями таких атак являются нарушение основной деятельности (36%) и утечки конфиденциальной информации (28%). Отличительной особенностью атак на госучреждения в этом регионе является то, что в основном их совершают APT-группировки (56%), надолго закрепляясь в инфраструктуре жертвы с целью кибершпионажа: такие злоумышленники имеют высокую квалификацию и располагают целым арсеналом вредоносного ПО и эксплойтов для компрометации систем и эксфильтрации данных. Интересный способ атаки с использованием методов социальной инженерии продемонстрировала группировка TA456: операторы создали фейковый профиль привлекательной девушки, в переписке с госслужащими завоевывали их доверие, а затем распространяли шпионское ПО.

Промышленные организации

Организации промышленного сектора формируют бóльшую часть ВВП стран Ближнего Востока, высоко оцениваются на рынке и аккумулируют большое количество конфиденциальных данных, тем самым привлекая к себе внимание злоумышленников: промышленность занимает вторую строчку самых атакуемых отраслей (16%). В 33% случаев преступники получают доступ к системам компаний-жертв в ходе атак на пользователей по каналам социальной инженерии; в 62% атак с использованием вредоносного ПО было замечено ВПО для удаленного управления, а также ПО, удаляющее данные (31%).

Актуальные объекты и методы кибератак на Ближнем Востоке

Деятельность APT-группировок и группировок вымогателей на Ближнем Востоке чаще всего была нацелена на конечные устройства и серверы: 78% кибератак на организации Ближневосточного региона было направлено на компьютеры, серверы и сетевое оборудование. Атаки на пользователей с использованием социальной инженерии (41% — доля организаций, 96% — частных лиц) являются одним из самых популярных методов атак: по данным годового исследования компании Verizone, человеческий фактор стал причиной более 80% взломов в 2022 году, в том числе и на Ближнем Востоке. Веб-ресурсы замыкают тройку наиболее атакуемых объектов в атаках на организации: злоумышленники эксплуатируют веб-уязвимости, похищают данные пользователей. Кроме того, веб-приложения являются целью дефейса и DDoS-атак со стороны хактивистов.

Рисунок 3. Объекты атак (доля атак)

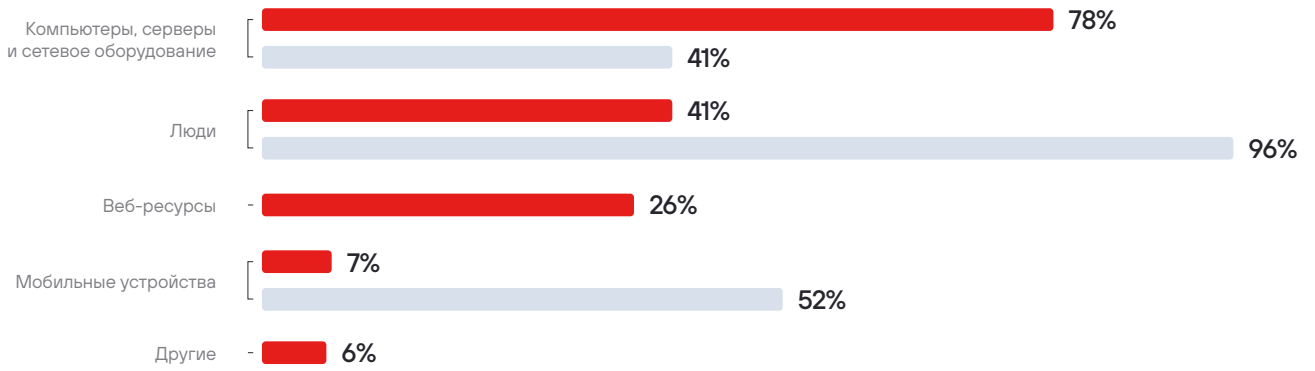
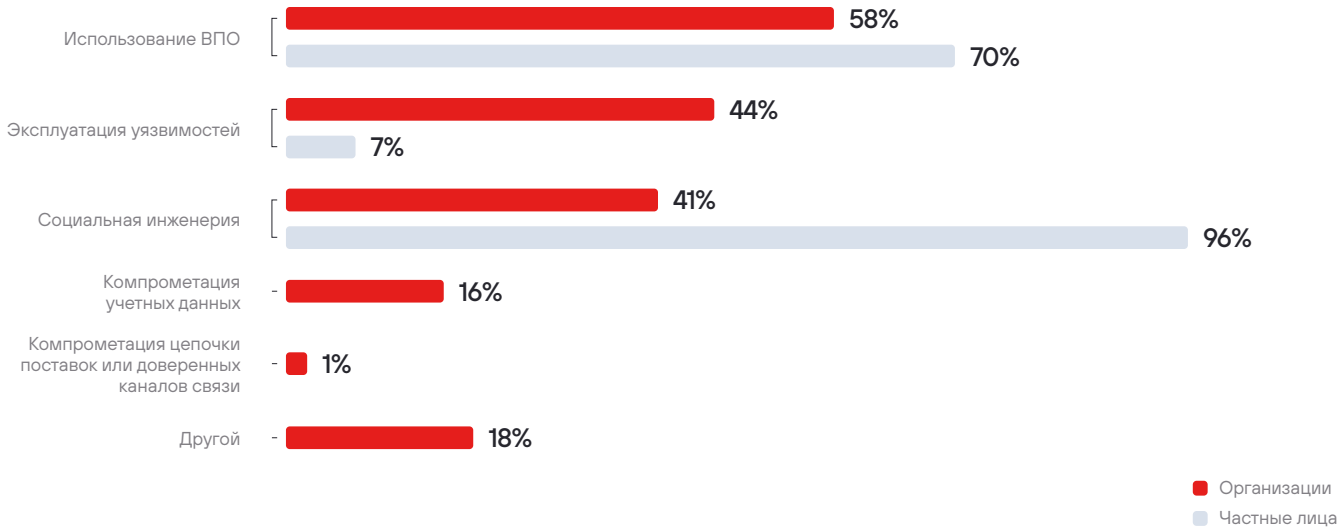
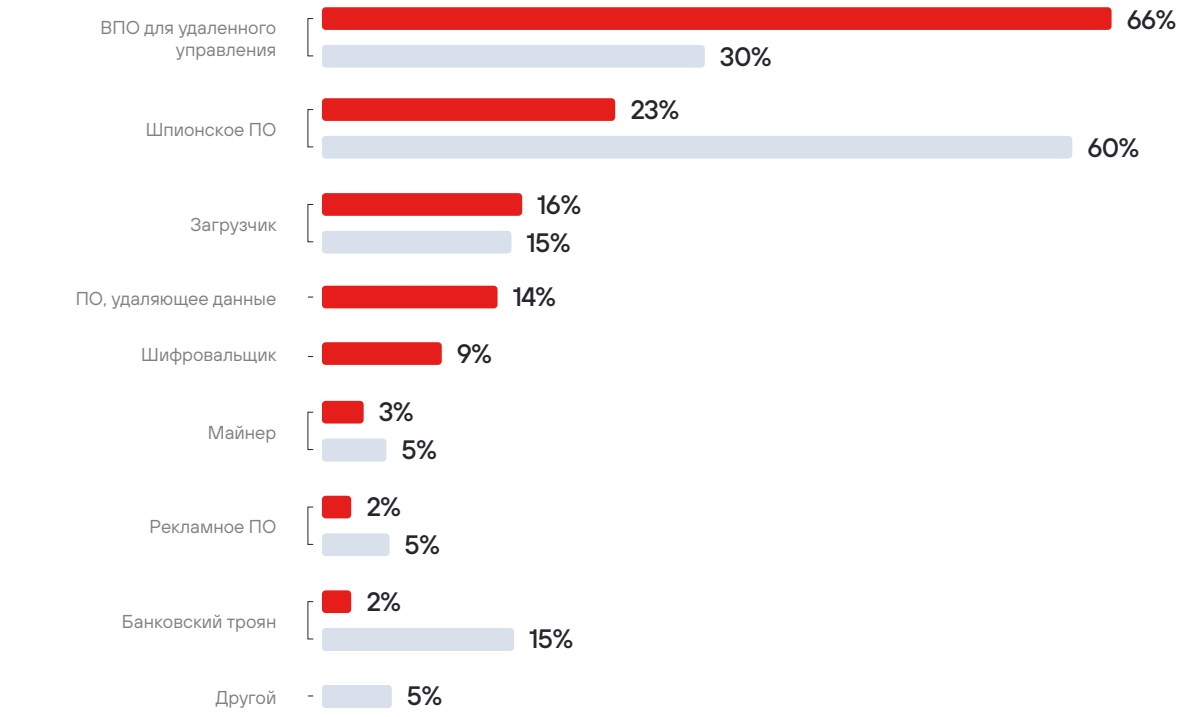


Рисунок 4. Методы атак (доля атак)



Вредоносное программное обеспечение в атаках на Ближнем Востоке

Рисунок 5. Типы вредоносного ПО (доля атак с использованием ВПО)



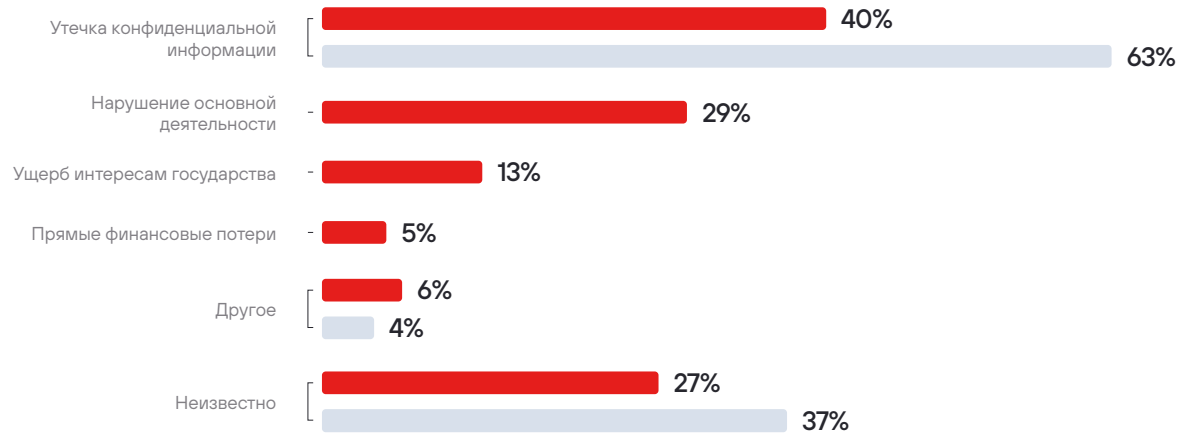
Практически две трети атак на организации в странах Ближнего Востока происходят с использованием различных типов вредоносного ПО. ВПО для удаленного управления стало самым популярным в таких атаках, и неспроста: оно предоставляет злоумышленникам практически полный контроль над скомпрометированным устройством, отключает средства защиты и обеспечивает постоянство пребывания в инфраструктуре. Этот вид вредоносов популярен среди всех злоумышленников, особенно у APT-группировок.

Шпионское ПО получило широкое распространение в атаках на частных лиц. Чаще всего злоумышленники распространяли его под видом легитимных приложений, например VPN-сервисов или приложений для создания виртуального номера.

Угроза со стороны группировок вымогателей является одной из главных во всем мире, в том числе и на Ближнем Востоке: активность операторов шифровальщиков в I квартале 2023 года возросла на 77% по сравнению с аналогичным периодом 2022 года. Согласно отчету Group-IB «Hi-Tech Crime Trends 2022/2023», наиболее атакуемыми странами в регионе Персидского залива стали ОАЭ (33%), Саудовская Аравия (29%) и Кувейт (21%).

Региональной особенностью Ближнего Востока является применение злоумышленниками вайперов. Вредоносы этого типа удаляют все пользовательские и системные файлы и выводят оборудование из строя. Особенно опасным случаем является попадание вайпера на устройства АСУ ТП, так как сбой в работе этого оборудования может привести к нарушениям технологического процесса и даже к аварийным ситуациям. Так, во II квартале 2022 года произошла крупная атака на три иранских сталелитейных завода, в результате которой были нарушены производственные процессы, а на одном из этих предприятий злоумышленникам удалось обрушить ковш с жидким чугуном, что вызвало пожар в цехе.

Рисунок 6. Последствия атак злоумышленников (доля атак)



Злоумышленники чаще всего были нацелены на кражу конфиденциальной информации и кибершпионаж (что соответствует общемировой тенденции к похищению данных), а также на нарушение основной деятельности организаций. Ввиду некоторой закрытости региона (случаи кибератак на Ближнем Востоке редко освещаются в открытых источниках) доля инцидентов, последствия которых остались неизвестны, остается достаточно высокой.

Рисунок 7. Типы украденных данных (в атаках на организации)

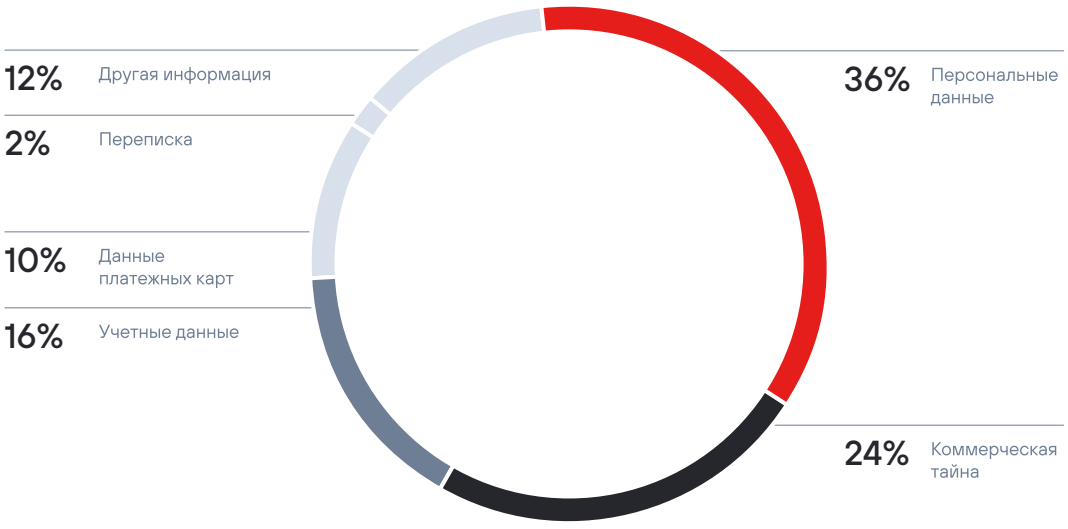


Рисунок 8. Типы украденных данных (в атаках на частных лиц)

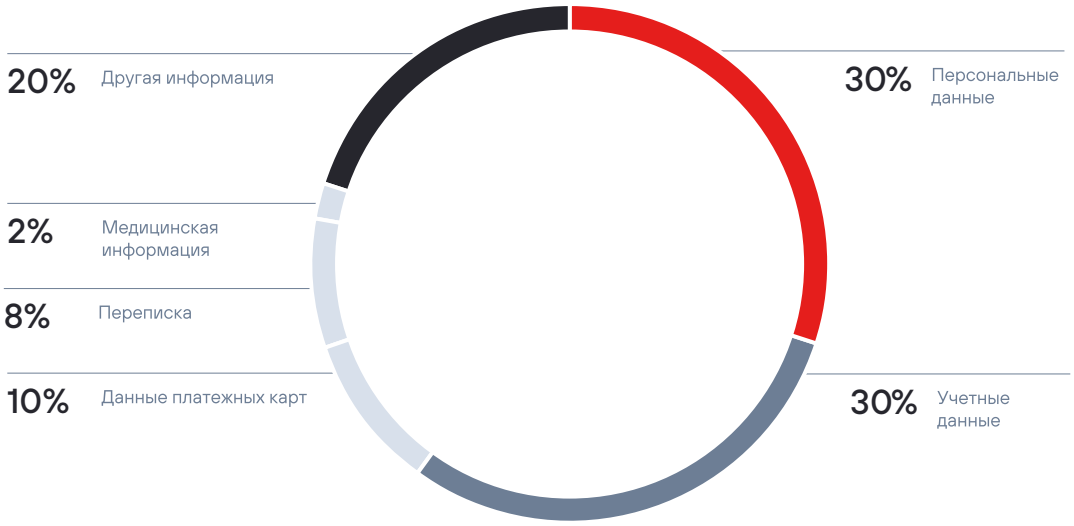


Рисунок 9. Группировки, атаковавшие организации и частных лиц на Ближнем Востоке

40%

успешных атак были совершены APT-группировками

APT-группировки
Организованные группы злоумышленников с высоким уровнем квалификации и технической оснащенности. Основная цель атак — кибершпионаж

Хактивисты
Злоумышленники, чьи кибератаки направлены не на получение финансовой выгоды, а на привлечение внимания общественности к различным социальным или политическим проблемам

Вымогатели
Злоумышленники, использующие вредоносное ПО для шифрования и эксфильтрации данных с целью дальнейшего вымогательства

Как решить проблемы кибер-безопасности на Ближнем Востоке

С точки зрения киберзащищенности Ближний Восток находится в потенциально уязвимом положении: богатый нефтью регион, страны которого ускоренными темпами проводят масштабную цифровизацию, внедряют инновационные технологии в процессы управления государством и важные отрасли экономики, в 2023 году станет одним из наиболее привлекательных для вымогателей, мошенников, APT-группировок и хактивистов. Основываясь на данных из открытых источников и на нашей статистике, можно сделать вывод, что большинство успешных кибератак на Ближнем Востоке осуществляется и будет осуществляться с помощью методов социальной инженерии, распространения и внедрения вредоносного ПО, эксплуатации веб-уязвимостей и уязвимостей в программном обеспечении.

Наиболее актуальными угрозами безопасности стран Ближневосточного региона в 2023 году являются:

- Кибератаки на правительственные организации. Злоумышленники (в частности, APT-группировки) могут направить свои усилия на компрометацию систем госучреждений, чтобы получить конфиденциальные данные, осуществлять кибершпионаж, нарушить деятельность или оказать влияние на принятие решений.
- Кибератаки на критически важную инфраструктуру. Эти атаки могут иметь самые серьезные последствия как для одной организации, так и для экономики или безопасности целой страны. Преступники могут избрать своими целями организации ТЭК, телекоммуникационные и финансовые учреждения, здравоохранение или транспорт.
- Фишинг и социальная инженерия. Атаки, основанные на фишинге и методах социальной инженерии, будут проводиться для получения доступа к системам организаций всех отраслей экономики, а также в отношении частных лиц.
- Распространение вредоносного ПО. Атаки с использованием вредоносов (трояны удаленного доступа, шпионское ПО, шифровальщики) останутся серьезной угрозой для организаций и отдельных пользователей.
- Хактивизм. Хактивисты могут использовать дефейс веб-ресурсов, DDoS-атаки или внедрение вредоносного ПО, чтобы нанести ущерб информационным системам и получить несанкционированный доступ к конфиденциальной информации. Кроме того, они способны вести киберпропаганду и распространять ложную информацию с целью влияния на общественное мнение.

Увеличение числа группировок и, следовательно, количества кибератак повысило потребность в обеспечении кибербезопасности организаций на Ближнем Востоке: согласно прогнозу International Data Corporation, расходы на обеспечение безопасности в регионе в 2023 году увеличатся почти на 8% в годовом исчислении, а наибольшая доля расходов (41%) придется на программное обеспечение.

Руководства стран Ближнего Востока в полной мере осознают серьезность киберугроз и создают нормативную базу для регулирования деятельности в киберпространстве:

- Катар внедрил положение для организаций в соответствии с законом о защите конфиденциальности персональных данных № 13 от 2016 года, чтобы обеспечить защищенность данных пользователей.
- Бахрейн ввел в действие закон о защите персональных данных (Personal Data Protection Law, PDPL) 1 августа 2019 года. Он был создан по образцу похожего документа, действующего в Европейском Союзе. Наказание для правонарушителей может составлять до 1 года лишения свободы.
- В ноябре 2021 года Объединенные Арабские Эмираты издали Федеральный закон № 45 (Закон ОАЭ о защите данных), который устанавливает более строгие стандарты конфиденциальности и защиты информации и определяет права и обязанности сторон в процессе обработки персональных данных.

Ввиду повышенной активности киберпреступников и серьезности последствий кибератак организации в странах Ближнего Востока должны уделять первоочередное внимание кибербезопасности. Им необходимо использовать инструменты, услуги и методики, которые могли бы расширить возможности мониторинга и реагирования на инциденты информационной безопасности, а также повысить осведомленность и бдительность их сотрудников для предотвращения кибератак. Одной из актуальных методик решения основных проблем является комплексный подход результативной кибербезопасности, который направлен на построение постоянной и автоматизированной системы защиты всей IT-инфраструктуры с учетом специфики деятельности и бизнес-процессов.

Для построения такой системы организациям необходимо выявить и оценить подлежащие защите информационные активы, а также определить недопустимые события — события, которые наступают в результате кибератаки и делают невозможным достижение операционных и (или) стратегических целей или приводят к значительному нарушению основной деятельности.

После того как активы и недопустимые события будут выявлены, следует провести мероприятия по оценке защищенности систем (киберучения, пентесты) и на практике реализовать (верифицировать) недопустимые события. По результатам оценки защищенности организации должны выбрать те компоненты защиты, которые позволят обеспечить три основные составляющие результативной кибербезопасности:

Мониторинг

Система безопасности в реальном времени должна определять, что происходит с защищаемыми активами и насколько соответствуют стандартам защищенности элементы инфраструктуры.

Внедрение систем класса SIEM (security information and event management) позволяет отслеживать и анализировать события безопасности, выявлять атаки и оценивать соответствие требованиям безопасности защищаемых элементов инфраструктуры. Для выявления атак в промышленных системах SIEM-решения могут дополняться специализированными продуктами для анализа трафика систем АСУ ТП: такие продукты отслеживают неавторизованные действия и активность вредоносного ПО без влияния на производственные процессы.

Реагирование

Система должна определять цель злоумышленника для быстрого и эффективного реагирования на инциденты, а также предотвращать наступление недопустимых событий.

Совместное использование решений классов XDR (extended detection and response) и SIEM дает возможность выявлять атаки в инфраструктуре и реагировать на них как вручную, так и в автоматическом режиме. Расширения возможностей обнаружения угроз и последующего реагирования можно добиться использованием песочницы для статистического и динамического анализа угроз, например выявления сложного вредоносного ПО. При проведении экспертных расследований инцидентов используются NTA-решения (network traffic analysis) для глубокого анализа трафика и обнаружения вредоносной активности. Также NTA-системы выступают в качестве сенсоров SIEM-решений для отображения информации о состоянии сети и выполняют роль инструмента для проактивного поиска угроз.

Управление активами

Одна из основных функций системы безопасности — постоянная инвентаризация активов и их классификация с учетом недопустимых событий и способов развития кибератак.

Системы класса VM (vulnerability management) автоматизируют процессы управления активами, выявления и исправления уязвимостей в элементах инфраструктуры в зависимости от степени опасности уязвимости. Также VM-системы отслеживают уровень защищенности инфраструктуры от эксплуатации уязвимостей, используемых в реальных атаках.

В случае, если компания занимается разработкой программных продуктов и веб-приложений, необходимо внедрять процессы безопасной разработки ПО и использовать средства анализа исходного кода для выявления уязвимостей и недостатков проектирования на этапе разработки.

Использование платформ bug bounty может помочь организациям построить процесс непрерывного анализа защищенности их сервисов и оптимизировать затраты на безопасность.

Сотрудники — главный актив организаций и в то же время один из основных векторов развития атак на корпоративные системы. Необходимо повышать уровень киберграмотности сотрудников (security awareness) при построении надежной защиты компании. Соблюдение правил цифровой гигиены снижает вероятность компрометации конечных точек. Пользователи, знающие актуальные угрозы, не будут вестись на уловки злоумышленников и открывать вложения из подозрительных электронных писем или подключать незнакомые устройства, а сообщат о подозрительной активности и попытках атак в SOC (security operations center).

Комбинация правильно настроенных средств защиты информации, непрерывности процессов и опытной команды специалистов по ИБ позволяет прийти к максимальной автоматизации и централизации управления безопасностью и достичь главной цели — защиты организации от недопустимых событий.

Об исследовании

Отчет содержит информацию об актуальных угрозах информационной безопасности Ближневосточного региона, основанную на собственной экспертизе компании Positive Technologies, а также на данных авторитетных источников. Под Ближним Востоком в отчете понимаются следующие страны: Бахрейн, Египет, Израиль, Иордания, Ирак, Иран, Йемен, Катар, Кипр, Кувейт, Ливан, Объединенные Арабские Эмираты (ОАЭ), Оман, Палестина, Саудовская Аравия, Сирия.

По нашей оценке, большинство кибератак не предается огласке из-за репутационных рисков. В связи с этим подсчитать точное число угроз не представляется возможным даже для организаций, занимающихся расследованием инцидентов и анализом действий киберпреступных группировок. Наше исследование проводится с целью обратить внимание компаний и обычных граждан, интересующихся современным состоянием информационной безопасности, на наиболее актуальные методы и мотивы кибератак, а также с целью выявить основные тенденции в изменении ландшафта киберугроз.

В рамках отчета каждая массовая атака (в ходе которой злоумышленники проводят, например, фишинговую рассылку на множество адресов) рассматривается как одна отдельная, а не как несколько. Термины, которые мы используем в исследовании, приведены в глоссарии на сайте Positive Technologies.

ptsecurity.com
pr@ptsecurity.com