White Paper

Руководство по угрозам кибербезопасности

Содержание

Введение	3
Фишинг	3
Вирусы-вымогатели	5
Криптомайнеры	7
Вредоносное ПО	8
Точки продаж	10
DDoS-атаки	11
Социальные сети	12
Угрозы для мобильных устройств	13
Веб-угрозы	14
Уязвимости	15
Угрозы IoT	16
Цепочки поставок	17
Контакты	19

Введение

Данное руководство формализует угрозы с которыми вы можете столкнуться и описывает, что можно сделать самостоятельно - и когда нужно обращаться за помощью экспертов по кибербезопасности.

Фишинг

Уровень угрозы:

Методы социальной инженерии и письма, содержащие вредоносные ссылки или вложения, являются распространенным способом, с помощью которого хакеры проникают в целевую среду. Фишинг обеспечивает более половины всех компрометаций в корпоративных сетях. Хакеры предпочитают этот метод атаки, потому что он основан на низкой осведомленности жертвы о кибергигиене, а также человеческом поведении и присущем ему доверии и любопытстве. Фишинг- это психологическая манипуляция в чистом виде и техники, которые аферисты использовали на протяжении тысячелетий.

Как происходит атака?

Сотрудники становятся жертвами фальшивых. но реалистично выглядящих электронных писем. Открытие вредоносных вложений, переход по ссылкам и ответы на такие письма, приводят к тому, сотрудники разглашают конфиденциальные данные (пароли, персональные данные и др. корпоративную информацию) или совершают ошибку при переводе финансовых средств.

Например, ваша бухгалтерия может получить по электронной почте поддельный запрос от Генерального директора на перевод средств контрагенту.

Что вы можете сделать?

Вы не столкнетесь с инцидентами, если ваши сотрудники смогут выявлять фишинговые письма.

Вы можете внедрять системы обучения кибергигиене и основам информационной безопасности. Вы также должны убедиться, что ваше программное обеспечение обновлено, чтобы избежать использования известных уязвимостей, а ваши сотрудники работают с наименьшим набором привилегий, необходимым для выполнения их должностных обязанностей.

Чем могут помочь эксперты?

Эксперты по информационной безопасности могут повысить эффективность ваши внутренних решений.

Например, они могут создать надежную образовательную программу по вопросам кибербезопасности, которая включает в себя инсценированные упражнения по борьбе с фишингом.

Они могут помочь вам управлять защитой через шлюзы электронной почты и веб-безопасности, которые могут блокировать вредоносные ссылки и вложения в режиме реального времени, а также предложить соответствующие средства управления политиками и фильтрами.

Вирусы-вымогатели

Уровень угрозы:

В последние годы количество атак с помощью вирусов-вымогателей резко возросло по одной простой причине - они работают.

Злоумышленники используют этот тип вредоносных программ для того, чтобы зашифровать корпоративную информацию до тех пор, пока жертва не заплатит выкуп (обычно к какому-то сроку). Даже в этом случае нет никакой гарантии, что злоумышленники не останутся во внутренней сети или действительно вернут доступ к вашим данным.

В некоторых случаях атаки нацелены именно на блокировку данных, а не на получение выкупа.

Как происходит атака?

Одной из самых вредоносных атак последних лет был червь-вымогатель, известный как WannaCry, который распространялся через уязвимость программного обеспечения для Windows, известную как EternalBlue.

Более распространенным примером может быть открытие одним из сотрудников вредоносного почтового вложения или переход по подозрительной ссылке, которая становится причиной проникновения вируса на устройство.

Что вы можете сделать?

Регулярно выполняйте резервное копирование важных данных и поддерживайте ПО и антивирус в актуальном состоянии.

Если вы все же стали жертвой атаки, немедленно отключите пораженную систему (скорее всего, рабочую станцию) от сети и начните процесс восстановления данных.

Чем могут помочь эксперты?

Специалисты по информационной безопасности могут вооружить вас проактивными решениями такими как:

- Тестирование на наличие уязвимостей;
- Системы защита от вредоносного ПО;
- Системы защиты электронной почты;
- Системы защиты конечных точек.

Продукты для защиты на конечных точек (EDR) мгновенно идентифицируют вирусы на основе вредоносных действий, которые они совершают.

Все эти решения могут помочь остановить атаки до того, как она приведут к ущербу.

Если вирус-вымогатель все-таки проник в вашу сеть, то эксперты помогут с минимизацией ущерба от атаки, проведут обучение по методам реагирования и расследованич инцидентов.

Криптомайнеры

По мере развития блокчейна все более дорогостоящими становятся вычисления, необходимые для создания новых цифровых монет. Злоумышленники решили: почему бы жертве не заняться добычей криптокоина?

Вредоносное ПО, которые крадет криптовалюту, эффективно только на компьютерах, хранящих такую валюту, но криптомайнеры, которые добывают валюту (обычно Monero) могут запускаться на любом устройстве, который они заразят. Преступники использую такое ПО, замедляя работу компьютера и тратя ресурсы на майнинг криптовалюты.

В то время как криптомайнеры должны быть установлены на устройсств, скрипты добычи, такие как Coin-hive, могут быть добавлены в код сайта. Однако, скрипты добычи имеют заметный недостаток. Они запускаются только в том случае, если браузер открыт и остается на сайте. Как только пользователь закрывает браузер или переходит на другой сайт, скрипт больше не работает.

Как происходит атака?

Злоумышленник воспользовался уязвимостями ПО или сотрудник открыл вредоносное вложение/ссылку, тем самым, установил вредоносное ПО.

Сотрудник посещает веб-сайт, который был взлома. Ресурсы компьютера пользователя начинают использоваться для генерации цифровых монет.

Что вы можете сделать?

Запустите антивирусное сканирование. Попробуйте определить, откуда идет нагрузка, чтобы убедиться, что криптомайнер является источником проблемы.

Используйте проверенные блокировщики рекламы и расширений браузера, которые специально блокируют скрипты криптомайнинга.

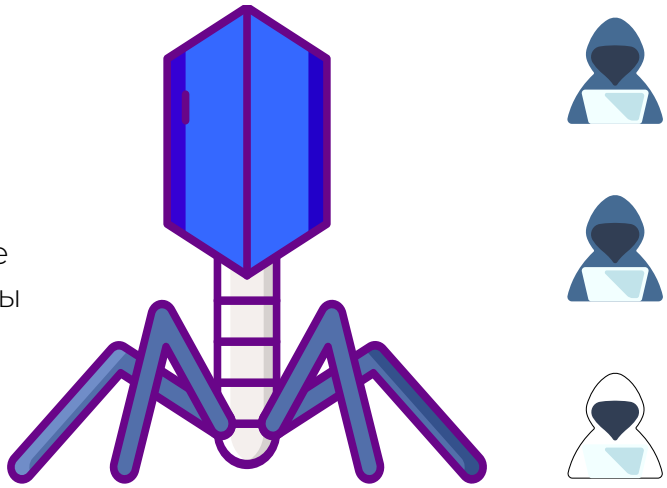
Чем могут помочь эксперты?

Антивирусное программное обеспечение обычно определяет и удаляет криптомайнеры. Но по мере того, как эта злоумышелнники улучшают вредоносное ПО, начинают появляться более опасные версии майнеров, которые ускользают от обнаружения. Компании по информационной безопасности помогут выбрать и внедрить современные средства защиты для противодействия сложным угрозам.

Вредоносное ПО

Уровень угрозы:

Важно помнить, что традиционные вредоносные программы, как правило, предназначенные для кражи данных все еще актуальны. Похитители паролей, банковские вредоносные программы, наборы инструментов для удаленного доступа и бэкдоры все еще широко распространены и остаются опасной угрозой.



К этой категории относятся и безфайловые вредоносные программы, которые могут получить контроль над компьютерами, используя обычные утилиты для сокрытия в памяти, тем самым уклоняясь от антивирусных программ, которые отслеживают жесткий диск.

Как происходит атака?

Злоумышленник может воспользоваться существующими уязвимостями программного обеспечения.

Пользователь попадается на фишинговое электронное письмо, которое заражает его компьютер.

Злоумышленник получает контроль над системой, обеспечивающий возможность несанкционированного доступ в любое время. Такие действия сложно обнаружить, потому что записи вредоносных файлов на жесткий диск не происходит.

Что вы можете сделать?

Убедитесь, что антивирусное программное обеспечение работает на всех устройствах, и настройте его на автоматическое обновление базы вирусов. Белый список - это еще один вариант, позволяющий запускать только предварительно утвержденные приложения.

Если вы подозреваете, что вредоносное программное обеспечение находится или находилось в системе, вы можете полностью переустановить ее, чтобы убедиться, что угроза была удалена.

Чем могут помочь эксперты?

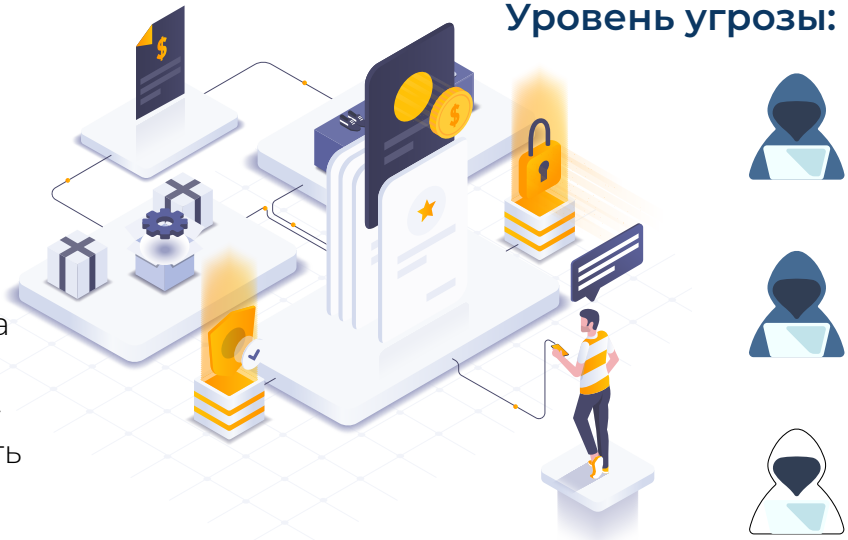
Чтобы справиться с более сложными вредоносными программами, созданными специально для того, чтобы избежать обнаружения обычными антивирусами, вам необходимо привлечь специалистов, которые смогут обеспечить надлежащую оценку рисков для вашей сети. Это поможет, лучше понять, как вам может угрожать вредоносное ПО.

Компании по информационной безопасности также могут вывести вас за рамки мер, ориентированных только на профилактику, внедрив системы обнаружения и реагирования на угрозы.

Кроме того, специалисты помогут выявлять аномалии в сети, расследовать инциденты, находить уязвимости и смягчать последствия инцидентов.

Точки продаж

Уровень угрозы:



Ритейлеры продолжают сталкиваться с заражениями POS-терминалов, а новые варианты вредоносных программ, нацеленных на платежные данные, такие как PinkKite и TreasureHunter, продолжают угрожать вашему бизнесу.

Вредоносные программы для POS часто находятся на взломанных терминалах в течение многих месяцев, прежде чем их обнаруживают.

Как происходит атака?

Как правило, злоумышленники и сканируют сеть на наличие уязвимых POS-систем и часто полагаются на стандартные или простые учетные данные для обычных утилит удаленного администрирования. Эти утилиты используются для выполнения легитимных функций управления на системах POS и программном обеспечении.

После того, как POS-система скомпрометирована, злоумышленники устанавливают вредоносные программы для сканирования, которые перехватывают данные платежных карт.

Также, злоумышленники, могут скомпрометировать устройства на этапах производства и поставки. Еще до того, как оно попадет конечному заказчику.

Что вы можете сделать?

Обычно злоумышленники компрометируют POS-системы с помощью средств удаленного сканирования и используют для взлома подбор простых паролей.

Используйте надежные пароли и по возможности отключайте удаленный доступ. Используйте сетевую сегментацию и ограничивайте веб-доступ на системах. Для большей уверенности проверьте поставщиков POS-терминалов, чтобы убедиться, что они серьезно относятся к безопасности.

Чем могут помочь эксперты?

Вы считаете, что ваши POS-системы безопасны? Единственный способ узнать наверняка - это привлечь экспертов для проведения сканирования уязвимостей и тестирования на проникновение.

DDoS-атаки

Уровень угрозы:

DDoS - атаки существуют уже несколько десятилетий, но их интенсивность только возрастает благодаря огромному количеству скомпрометированных IoT-устройств. Помимо массированных нападений, более короткие и малообъемные атаки иногда отвлекают внимание от более серьезных сетевых вторжений.

Как происходит атака?

Чтобы перегрузить серверы и сделать веб-сайт неработоспособным засоряют канал большим объемом трафика. При удачной атаке на вашу компанию, клиенты не смогут воспользоваться сайтом или другими ресурсами. Вы будете испытывать сбои в работе файловых серверов и других систем.

Что вы можете сделать?

Компании должны серьезно относиться к DDoS-атакам. Необходимо проактивно проверять системы периметровой защиты, чтобы определить, какой трафик вы пропускаете внутрь и наружу и подтвердить способность остановки нелегитимного трафика на периметре.

Чем могут помочь эксперты?

Компании по информационной безопасности помогут внедрить современные средства защиты от DDoS-атак, а также окажут услуги по минимизации последствий инцидента и помогут справиться с массированными вторжениями.

Социальные сети

Уровень угрозы:

Социальные сети часто являются игнорируемым вектором атак. Они не только являются основной территорией для распространения вредоносных программ и других мошеннических схем, но и служат инструментом получения информации для дальнейших фишинговых атак и социальной инженерии.

Как происходит атака?

Остерегайтесь чрезмерной активности сотрудников в социальных сетях. Например, упоминание подробностей рабочей поездки могут быть использованы злоумышленниками для создания успешной фишинговой атаки. Также, возможна ситуация, когда сотрудник по ошибке публикует конфиденциальную информацию в социальной сети.

Что вы можете сделать?

Запрет на использование социальных сетей практически нереализуем, учитывая, насколько тесно они вплетены в нашу личную и деловую жизнь.

Вместо этого, обратитесь к разработке и внедрению политик использования социальных сетей, а также обучению сотрудников основам информационной безопасности. Следите за аккаунтами сотрудников в социальных сетях на предмет признаков утечки информации, компрометации или другой нелегитимной деятельности.

Чем могут помочь эксперты?

Компании по информационной безопасности помогут внедрить DLP системы, предотвращающие утечку данных в т.ч. через социальные сети и мессенджеры. Внедрить шлюзы веб-безопасности и решения по мониторингу активности сотрудников в социальных сетях.

Угрозы для мобильных устройств

Уровень угрозы:

Сегодня мобильные устройства - неотъемлемая часть как личной, так и деловой жизни сотрудников. Предприятия могут получить огромную выгоду от использования мобильных устройств в работе. Однако, есть и очевидные риски, включая мошенничество, а также вредоносные приложения, установка которых может привести к компроментации корпоративной инфраструктуры и сетевым атакам.

Как происходит атака?

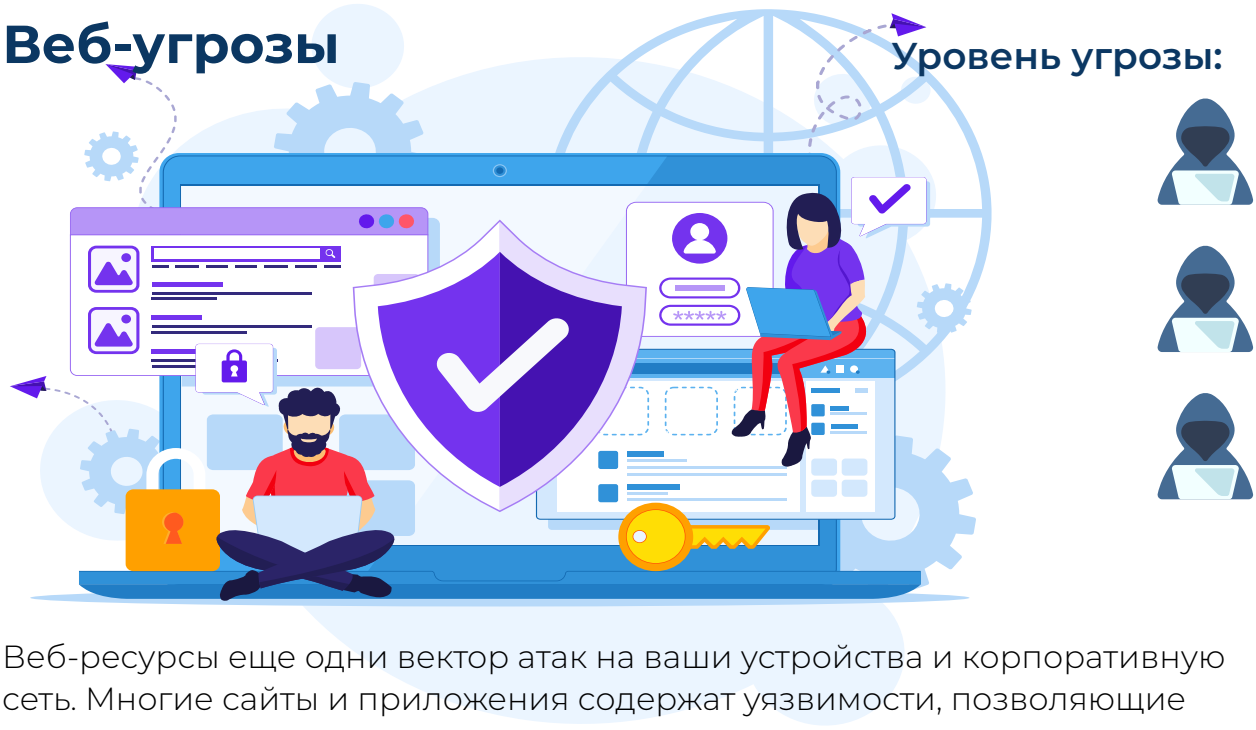
Сотрудник получает сообщение, содержащее ссылку или скачивает приложение. Оно оказывается вредоносным и дает злоумышленникам доступ к данным, которые можно использовать для входа в корпоративную сеть.

Что вы можете сделать?

Вы должны разработать и внедрить политики мобильной безопасности, которые будут включать регламенты по установки приложений и использованию общедоступных сетей. Кроме того, необходимо внедрить функциональные возможность стирания корпоративных данных в случае утери мобильного устройства.

Чем могут помочь эксперты?

Компании по информационной безопасности проведут тестированичя на проникновения и оценять уровень защиты мобильных устройств. Эксперты могут усилят ваши возможности по оценке рисков, управлению устройствами и защиты от вредоносного ПО внедрением систем MDM, защиты конечных устройств и DLP систем.



Веб-ресурсы еще одни вектор атак на ваши устройства и корпоративную сеть. Многие сайты и приложения содержат уязвимости, позволяющие злоумышленникам скомпроментировать сеть.

Как происходит атака?

Злоумышленник сканирует ваш сайт, обнаруживает, например SQL-уязвимость, и использует ее для проникновения в корпоративную сеть.

Что вы можете сделать?

Если вы создаете и администрируете веб-ресурсы собственными силами, вы должны собрать команду, которая компетентна в области безопасности и обучена эффективному обслуживанию веб-ресурсов, поиску и устранению уязвимостей. Другой вариант - внедрить программу Bug Hunting, с помощью которой пользователи получают компенсацию за обнаружение уязвимостей.

Чем могут помочь эксперты?

Компании по информационной безопасности помогут провести тестирования на проникновения и оценить реальную систуацию с защитой веб-русерсов. Помогут внедрить многоуровневую стратегия защиты. Поставить и настроить межсетевые экраны веб-приложений (WAF), системы выявления аномального поведения и защиты от целевых атак, чтобы помочь клиентам оставаться обезопасить себя от широкого спектра современных угроз.

Уязвимости

Уровень угрозы:

Даже если вы создаете приложение, используя безопасные платформы, технологии и принципы разработки, регулярно обновляете программное обеспечение на конечных устройствах и других корпоративных ресурсах одна уязвимость, неправильная конфигурация или настройка может дать злоумышленнику возможность компрометации вашей сети. Помните, что злоумышленники могут позволить себе совершить много ошибок, так как они ищут всего лишь одну оплошность, которую вы допустили при защите своей инфраструктуры.

Как происходит атака?

Вы по ошибке активируете гостевой доступ при добавлении нового пользователя.

Сотрудник добавляет новые правила межсетевого экрана, которые оставляют больше портов открытыми, чем допускает политика информационной безопасности.

Что вы можете сделать?

Исправляйте известные уязвимости и регулярно обновляйте программное обеспечение и устройства. Внедрите систему управление для отслеживания всех изменений, внесенных в вашу информационную инфраструктуру.

Чем могут помочь эксперты?

Эксперты помогут регулярно проводить внешнее и внутреннее сканирование для проактивного поиска и помощи в устранении уязвимостей. Проведут тестированияе на проникновение и редтиминг для оценки эффективности систем безопасности компании. Модернизирует инфраструктуру и решения по информационной безопасности.

Угрозы IoT

Угрозу вредоносных программ для Интернет вещей (IoT) часто не считают серьезной угрозой. Отчасти из-за того, что их не воспринимают в качестве традиционной уязвимой конечной точки. Но есть о чем беспокоиться!

Каждая конечная точка или актив, подключенный к Интернету, начиная с маршрутизаторов и заканчивая умными колонками, потенциально добавляет еще один вектор атаки. Что делает устройства Интернета вещей (IoT) особенно опасными.

Как происходит атака?

Помимо использования уязвимостей программного обеспечения устройств Интернета вещей (IoT) для прямого воздействия на ваш бизнес, злоумышленники также могут использовать скомпрометированное устройство, чтобы закрепиться в вашей внутренней сети.

Что вы можете сделать?

Зачастую, производители устройств IoT не рассматривают информационную безопасность, как приоритетную задачу. Узнайте как можно больше об установленных устройствах, о том, как они осуществляют работу с данными, их сбор и отправку, и как они защищены. Были ли инциденты с компроментацией устройств? Используйте надежные пароли и поместите устройство за корпоративным межсетевым экраном и, возможно, в защищенный сегмент, предназначенный для потенциально опасных IoT. Регулярно обновляйте устройства.

Чем могут помочь эксперты?

Воспользуйтесь помощью экспертов, чтобы обнаружить и протестировать слабые места в информационной инфраструктуре (в частности IoT-устройствах), а также эффективно контролировать и защищать сетевые активы.

Цепочка поставок

Уровень угрозы:

Поставщики, партнеры и контрагенты представляют реальную опасность, если их системы информационной безопасности не работают должным образом. Практика учит обращать пристальное внимание на риски и угрозы третьих лиц.

Как происходит атака?

Поскольку цепочка поставщиков и контрагентов обширна, атаки на supply chain становятся все опаснее. Инциденты могут варьироваться от взлома компании аутсорсинга юридической помощи с целью кражи конфиденциальной информации о клиентах до атаки на вашего поставщика с целью компроментации оборудования и программного обеспечения, которое вы используете.

Что вы можете сделать?

Узнайте о политиках безопасности поставщиков и контрагентов. По возможности, согласуйте стандарты, которым они должны соответствовать. Настройте сетевую сегментацию, чтобы продукты, которым вы не полностью доверяете никогда не касалась более чувствительных частей корпоративной сети.

Чем могут помочь эксперты?

Эксперты помогут правильно оценить риски информационной безопасности. И если эта оценка выявит явные недостатки, эксперты проверят корпоративную инфраструктуру на уязвимости. Зачастую, бизнес медленно реагирует на атаки через компроментацию цепочки поставщиков. Компании по информационной безопасности помогут обеспечить эффективное реагирование и устранение инцидентов.

Чем мы можем Вам помочь?

ООО «НТЦ ЕВРААС», являясь многопрофильной коммерческой структурой, имеет все необходимые лицензии регуляторов рынка информационной безопасности, в том числе лицензии на осуществление работ с использованием сведений, составляющих государственную тайну.

Обладая фундаментальными знаниями и опытом в области защиты информации, эксперты НТЦ «ЕВРААС» предлагают новейшие комплексные решения в сфере кибербезопасности.

Мы проектируем системы под конкретные нужды и специфику организаций, тем самым гарантируя, что система информационной безопасности комплексно решает все задачи и обеспечивает надежную круглосуточную защиту ваших корпоративных ресурсов и данных.

Контакты:

г. Москва, ул. Автозаводская 13/1

8 (495) 748-09-44

evraas@evraas.ru

При подготовке материала, в частности, использовалась информация сайта Trustwave.