Защита от программ-вымогателей

Рекомендуемые практики

Время для глубокой обороны

AON

Оглавление

Программы-вымогатели: Время для глубокой обороны

Программы-вымогатели быстро становятся доминирующим инструментом у кибер-преступников, которые те используют, чтобы получить как можно больше от своих жертв посредством двойной угрозы - парализации бизнес-систем и использования украденных конфиденциальных данных для последующего вымогательства. Но готовы ли организации к противостоянию этой угрозе? Согласно отчету Aon о кибер-безопасности за 2021 год, только 31% опрошенных сообщают о наличии в организации адекватных мер по обеспечению устойчивости бизнеса к воздействию вымогательского ПО[1].

Программы-вымогатели представляют собой критический риск для современного бизнеса; причем частота, сложность и влияние на деловую активность организаций атак таких программ значительно возросли за последние годы. Вредительское ПО наносит значительный финансовый ущерб, нарушает деловые процессы и подрывает репутацию. Методы, используемые злоумышленниками, не стоят на месте, не должны отставать и методы защиты. В борьбе с программами-вымогателями необходимо применять глубинный подход, идущий в ногу с достижениями отрасли. Причем вышеуказанное не ограничивается техническими мерами: убытки, связанные с программами-вымогателями, также оказывают влияние на рынок кибер-страхования.

Рекомендуемые практики Aon по защите от вымогательского ПО Данные методы разработаны с целью помочь организациям понять, какие меры контроля необходимы, и определить общие и доступные способы защиты от атак.

Проактивное участие руководителей или технических специалистов в выполнении приведенных рекомендаций может помочь в эффективном противодействии вредоносному ПО на все более сложном рынке кибер-страхования.

Хотя и меры контроля регулярно согласуются с рисками и технологическими возможностями, невозможно добиться устойчивости только за счет развертывания приведённых мер контроля, и каждая защитная мера должна стать частью более широкой стратегии кибер-безопасности, включающей управление, технические средства контроля, риски и финансовые механизмы, основанные на понимании относительного кибер-риска.

Настоящие рекомендации были разработаны на основе более чем 20-ти летнего практического опыта предоставления кибер-решений, а также с использованием отраслевых практик и структур. Цель данного руководства заключается в консолидации средств контроля, которые могут положительно повлиять на кибер-защиту организации, необходимую для управления угрозами со стороны программ-вымогателей. Каждая из рекомендуемых практик соответствует категориям, определенным Рамочной программой кибер-безопасности Национального института стандартов и технологий (NIST): Идентификация, Защита, Обнаружение, Реагирование и Восстановление.

Смягчение последствий угроз от вымогательского ПО Устойчивое развитие требует многофункционального комбинированного подхода, и успех в одной области не может компенсировать недостаток в других. Истинного универсального решения на данный момент не существует. Комплексный подход компании Aon к управлению угрозами от вымогательского ПО включает в себя три ключевых этапа: оценку, смягчение и передачу - элементы управления, описанные в данном документе, соответствуют фазе смягчения.

Контрольный список защиты от программ-вымогателей Aon может помочь вам оценить текущие возможности вашей компании по шкале зрелости от "начального" до "продвинутого" уровня. Показатель общей зрелости защиты от вымогательского ПО можно получить, заполнив контрольный список, в котором также будут выделены ключевые области для совершенствования.

В поддержку необходимых усовершенствований и в соответствии с этими рекомендациями компания Aon объединила важнейший опыт, возможности и данные ключевые рекомендации для разработки пакета мер защиты от программ-вымогателей, призванного помочь усилить защитные меры, необходимые для углубления подхода при управлении рисками от вымогательского ПО. Чтобы узнать больше, свяжитесь с локальным представителем Aon.

1. Aon's 2021 Cyber Security Risk Report https://www .aon .com/2021-cyber-security-risk-report/

Природа программ-вымогателей меняется

Согласно прогнозам, глобальные убытки от программ-вымогателей, которые станут наиболее быстрорастущим видом кибер-преступности, с которыми столкнутся организации в 2021 году, достигнут 20 миллиардов долларов США, что более чем **в 50 раз больше**, чем 5 лет назад.[2]

Рост числа атак программ-вымогателей происходит по экспоненте. С появлением феномена "программы-вымогатели как услуга", организациям стало еще сложнее им противостоять, поскольку преступники обмениваются инструментами взлома и продают вредоносное ПО между группами. Общая стоимость ущерба, связанного с программами-вымогателями, вероятно, даже выше, чем сообщается, поскольку жертвы часто хранят молчание и выплачивают выкуп без лишней огласки, а злоумышленники не всегда публикуют данные, полученные из скомпрометированных сетей.

Ни государственный сектор, ни частные организации, независимо от размера или отрасли, не защищены на 100%. И, при всем этом, многие организации до сих пор имеют лишь базовый уровень защиты. А сейчас, как никогда, актуально внедрение проактивной защиты, поскольку злоумышленники переходят от тактики "пальбы наугад" к снайперской стрельбе и охоте на крупную дичь. Угроза для организаций заключается не только в шифровании и прерывании деловой активности, но и в возможности раскрытия хакерами похищенных конфиденциальных данных.

Миф об атаке нулевого дня

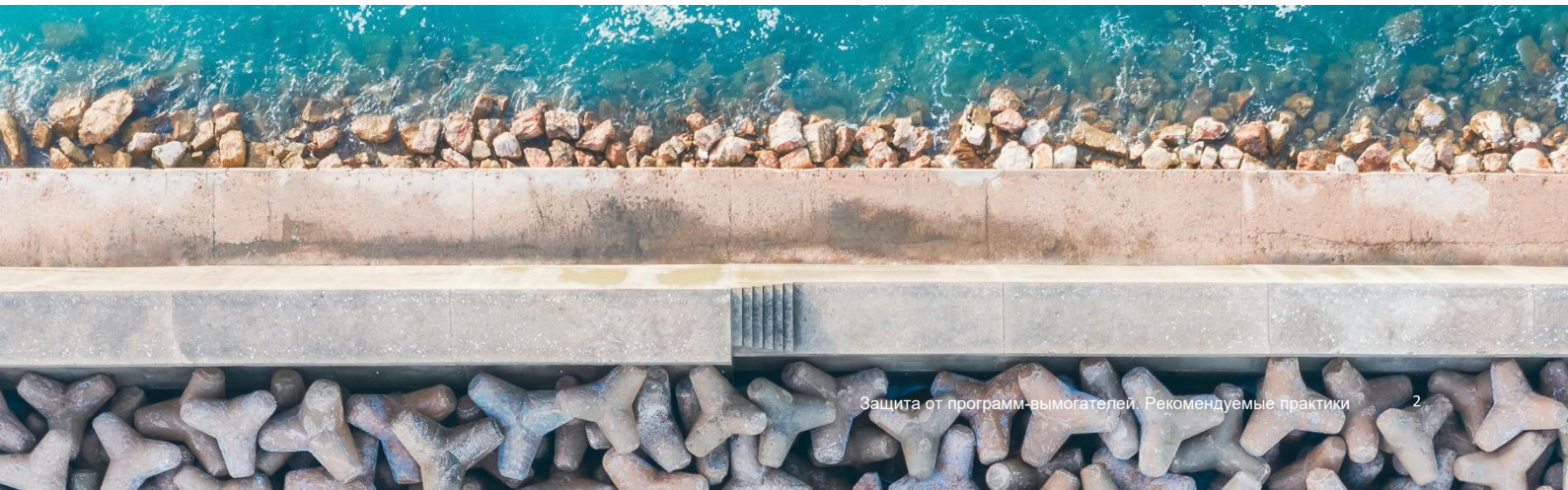
Ошибочно полагать, что злоумышленники концентрируются на уязвимостях нулевого дня и получают доступ к сети только в момент начала атаки. Злоумышленники, скорее всего, получили доступ к сети гораздо раньше, используя это время для проведения разведки и создания учетных записей администраторов для повышения своих привилегий. Чтобы получить постоянный доступ при проведении атаки, они отключают правила брандмауэра, активируют удаленный доступ к серверу и даже создают постоянный черный ход в сеть, обходя обычную аутентификацию или шифрование. Еще до того, как атака произойдет, они часто уже имеют в распоряжении отфильтрованные данные как для доказательства того, что у них есть доступ, так и для угрозы разоблачения.

Ставки повышаются

Тактики двойного вымогательства развенчали миф о возможности полагаться на резервные копии в борьбе с требованиями вымогателей. Злоумышленники все чаще выбирают цели не только потому, что они в курсе каких-либо их уязвимостей, но и потому, что они предчувствуют большую выгоду от утечки данных.

Даже если резервные копии не были скомпрометированы и их можно будет использовать для восстановления сервисов, злоумышленники все равно имеют козырь в рукаве, чтобы заставить жертву заплатить выкуп, выборочно публикуя конфиденциальные данные в качестве рычага вымогательства. Выполнение требования об оплате выкупа для получения доступа к ключам дешифровки не гарантирует защиты от последующей утечки данных. Известны случаи, когда выкуп был оплачен, а преступники впоследствии монетизировали извлеченные данные, продавая их на аукционе в dark web.

2.https://cybersecurityventures.com/global-ransom-ware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/



Страховые компании на грани перемен

Сейчас страхование является ключевым оружием арсенала организаций в борьбе с вымогательским ПО. Но резкое увеличение **частоты и серьезности убытков, связанных с вымогательским ПО, изменило рынок кибер-страхования.**

Страховые компании требуют от организаций все больше информации для андеррайтинга для гарантии готовности последних к атаке программ-вымогателей и наличия у них соответствующих уровней зрелости средств контроля безопасности.

Подобно тому, как страхование имущества требует принятия соответствующих мер противопожарной безопасности, кибер-страхование также применяет соответствующие меры кибер-гигиены. Демонстрация упреждающих стратегий снижения рисков, таких, как оценка и тестирование, теперь имеет решающее значение как для лучшего позиционирования риска для страховщика, так и для обеспечения безопасности.

Страховщики проверяют уязвимость для программ-вымогателей с помощью специальных дополнительных вопросников и технологий сканирования. Теперь они сосредоточены на планировании непрерывности деловой активности и аварийного восстановления, контроле привилегированного доступа, многофакторной аутентификации, проактивном сканировании / тестировании и общей готовности к реагированию на инциденты.

Кроме того, страховщики регулярно корректируют свой подход к андеррайтингу, пересматривают условия страхования и свои емкости. Конкретные примеры страхового покрытия, на которые страхователям придется ориентироваться, приведены в обзоре Aon 2021 Cyber Insurance Snapshot,[3] но вывод для организаций заключается в том, что стратегический подход к брокерской деятельности, основанный на оценке рисков, имеет решающее значение на жестком рынке кибер-страхования. Тщательная предандеррайтинговая подготовка организации жизненно важна для того, чтобы выделиться на рынке и сохранить доступ к емкостям страховщиков. Страховые компании постоянно повышают планку в отношении рисков, которые они принимают на страхование. То, что может пройти проверку в этом году, совсем не обязательно пройдет ее в следующем.

Чтобы опередить угрозу и оставаться привлекательным риском для страховщиков, организации должны постоянно повышать свой уровень кибер-безопасности и быть готовыми рассказать свою историю страховщикам, а также способствовать возможности долгосрочного партнерства на рынке, которое может иметь крайне высокое значение. Кибер-страхование является важной мерой по снижению рисков для корпоративного баланса, что означает, что необходимо развивать и поддерживать необходимый уровень прозрачности в отношениях со страховыми партнерами со стороны предприятия (и наоборот).

3. Aon's 2021 Cyber Insurance Snapshot https://www.aon.com/cyber-solutions/thinking/aons-cyber-insurance-snapshot-emea/

Сейчас страховщики наблюдают увеличение частоты и серьезности убытков, связанных с программами-вымогателями, поэтому **организациям следует быть готовыми продемонстрировать свою готовность** к атаке такого ПО.

Программы-вымогатели. Оценка рисков

Программы управления рисками должны **строиться на основанном на данных подходе,** который оценивает потенциальные уязвимости как на уровне системы, так и на уровне человеческого фактора.

Многие организации будут вкладывать средства в программы управления кибер-рисками, поэтому важно рассмотреть вопрос согласования. Отраслевые структуры, такие, как NIST Cyber Security Framework, предоставляют определенные профили, которые можно использовать для оценки, смягчения и управления рисками, связанными с программами-вымогателями, и демонстрируют важность систематического выявления рисков в масштабах предприятия до принятия мер по исправлению и защите от этих проблем.

В силу постоянства роста угроз, циклический подход к оценке улучшит представление организации о критически важных активах и позволит легко продемонстрировать слабые места в программе, что обеспечит план для принятия лучших решений: будь то приоритезация уязвимостей, частота исправлений или инвестиции в новые технологии для достижения целей снижения риска. Другой проблемой для многих организаций является создание устойчивой методологии для облегчения процесса, который может включать несколько направлений работы. Например, не имеет смысла отделять оценки кибер-безопасности от заявлений о страховании или дополнительных наборов вопросов по программам-вымогателям.

Организации должны адаптировать процессы для экономии времени и максимизации производительности. Страховой полис должен стать естественным дополнением к стратегии безопасности. Это означает, что если он не подходит и не работает параллельно с отделами ИТ и информационной безопасности, то стоит задуматься о его целесообразности в общем. Кроме того, согласование с корпоративными реестрами рисков и обеспечение понимания на уровне руководства стратегической программы инвестиций в безопасность позволит усовершенствовать общие протоколы управления, связанные с постоянным совершенствованием и повышением устойчивости протекания деловой активности.

"Есть только два типа компаний: **те, которые были взломаны, и те, которые будут.** Что по сути можно объединить в одну категорию: те, которых уже взламывали и те, кого взломают снова".[4]

Роберт Мюллер
Бывший сотрудник Федерального бюро расследований

4. https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

Рекомендуемые практики

Готовность к противодействию атакам программ-вымогателей требует зрелого и продуманного подхода, **использующего соответствующие средства управления людьми, процессами и технологиями.** Многие области управления могут быть техническими по своей природе, но для достижения устойчивости требуется согласование с руководством, владельцами рисков и бизнеса.

Кроме того, средства контроля не следует рассматривать как отдельные возможности, а скорее, как неотъемлемые меры, являющиеся частью более широкой защиты предприятия от кибер-угроз, и в особенности в отношении вымогательского ПО.

Эти рекомендации отражают сочетание практического опыта, лучших отраслевых практик и отзывов ведущих партнеров в области кибер-безопасности и страхования, однако они также соответствуют профилю ***NIST Cybersecurity Framework Profile для управления рисками вымогательского ПО***. Цель этих рекомендаций - это не зеркальное отражение тех мер контроля, которые описаны в данном стандарте, а консолидация и осмысление более чем 20-летнего опыта Aon в разработке кибер-решений, чтобы предоставить организациям четкое и практическое руководство, которое они могут использовать для защиты своего бизнеса от кибер-атак.

В этих рекомендациях рассматриваются области кибер-контроля, которые могут быть полезным инструментом для понимания готовности организации не только к реагированию, но и для предоставления структуры сквозного управления кибер-рисками: ***определение, защита, обнаружение, реагирование и восстановление.***

Определение	Защита	Обнаружение	Реагирование	Восстановление
Понимание и оценка рисков, которые представляют для вашей организации программы-вымогатели.	Разработка защитных мер для предотвращения угроз программ-вымогателей.	Выявление и обнаружение событий и инцидентов кибер-безопасности до начала реагирования.	Принятие мер реагирования в случае кибер-инцидента.	Возвращение к работе и минимизация последствий кибер-инцидента.

Определение

Понимание и оценка рисков, которые представляют для вашей организации программы-вымогатели.

Меры контроля, которые необходимо рассмотреть:

Понимаете ли вы профиль атаки вашей организации и проанализировали ли вы процедуры управления, контроля, роли и обязанности персонала?

Проверили ли вы свой уровень защиты, проанализировав средства контроля безопасности ключевых систем?

Функция *определения* представляет собой понимание и оценку рисков, которые вымогательское ПО представляет для организации, что может означать понимание технологического комплекса организации, ролей и обязанностей, а также безопасности ключевых бизнес-систем. Эти сведения помогают сформировать основу, необходимую для создания и управления соответствующими механизмами защиты, необходимыми для снижения риска программ-вымогателей. В рамках оценки организациям следует обратить внимание на то, как осуществляется резервное копирование данных и может ли организация восстановить данные в случае атаки на системы, хранящие эти данные.
Для защиты от программ-вымогателей крайне важно, чтобы организации понимали свой профиль атаки и тестировали средства управления системами.

Чтобы понять профиль атаки организации: Проанализируйте управление, контроль, роли и обязанности
Для того, чтобы управлять риском, важно сначала понять его. Выходя за рамки общей оценки кибер-рисков (которая рекомендуется в рамках надлежащей гигиены безопасности и обеспечивает полезную оценку кибер-рисков), Aon рекомендует организациям понимать свой профиль атаки, поскольку он может иметь отношение к инцидентам с использованием программ-вымогателей. Это означает оценку систем и данных, на которые организация полагается при ведении бизнеса, возможные уязвимые точки атаки технологического комплекса и степени зрелости соответствующих средств защиты, особенно для потенциального воздействия программ-вымогателей.

Принимая во внимание структуру (такую как NIST), имеющую определенный профиль для программ-вымогателей, Aon рекомендует организациям провести обзор управленческого персонала, задействованного в кибер-безопасности, и определить, кто несет ответственность, подготавливает отчеты, проводит консультации и предоставляет информацию (RACI) при управлении рисками от программ-вымогателей. Это поможет не только при проведении защитных / оборонительных мероприятий, но и при планировании и восстановлении после них. Оценка риска должна также учитывать управление активами, управление рисками и влияние, которое могут оказать третьи стороны на порядок атаки на организацию. Понимание уровня зрелости существующих механизмов контроля может помочь в вопросе распределения инвестиций в требуемых областях безопасности.

Проверка средств защиты: Рекомендуется проверить защитные средства контроля безопасности ключевых систем
В дополнение к оценке зрелости средств контроля и более глубокому пониманию точек атаки на организацию, Aon рекомендует провести тестирование безопасности ключевых бизнес-систем для выявления уязвимостей и проверки вероятности потенциальной атаки с использованием программ-вымогателей. Частично это может быть достигнуто за счет постоянного сканирования уязвимостей и управления ими, однако, этого можно добиться и с помощью целевых мероприятий, направленных на тестирование безопасности. Хотя точная цель такого тестирования будет зависеть от систем в организации и связанной с ними критичности, типичные рекомендуемые системы для оценки включают Active Directory, Office 365, корпоративные почтовые системы и тестирование корпоративной сборки или "конечной точки". Эти рекомендации даны в связи со способом распространения программ-вымогателей (часто запускаемых через электронную почту / конечные точки) и связанные с ними системы. Учитывая, что защитные механизмы в рамках этих целей будут обеспечивать начальную линию защиты, Aon рекомендует оценить их эффективность до того, как это сделает злоумышленник.

Защита

Разработка защитных мер для предотвращения угроз программ-вымогателей.

Меры контроля, которые необходимо рассмотреть:

Развернули ли вы управление привилегированным доступом (PAM) и внедрены ли элементы управления многофакторной аутентификацией (MFA)?

Повышаете ли вы осведомленность сотрудников о кибер-безопасности, например, с помощью симуляции фишинга?

Есть ли у вас адекватный план реагирования на инциденты, и как давно вы его проверяли?

Функция *защиты* сосредоточена на разработке соответствующих защитных мер, необходимых для управления рисками, вскрытыми на шаге обнаружения. В частности, это означает защиту людей, технологий и данных в бизнесе, развертывание критически важных инструментов безопасности и подготовку к реагированию на инциденты.

Управляйте рисками с помощью средств контроля личности
Бизнес-пользователи часто становятся первой точкой атаки злоумышленников, и поэтому защита от первоначального взлома учетной записи может стать первой линией обороны. Возможности управления идентификацией и доступом (IDAM) сосредоточены на предоставлении авторизированным пользователям доступа к нужным системам по определённым причинам и безопасным способом. Поскольку программа-вымогатель распространяется, отслеживая доступ зараженного пользователя / конечной точки и шифруя связанные файлы и бизнес-системы, управление доступом пользователей и аутентификация могут иметь важное значение для предотвращения, а также для противодействия атаке программы-вымогателя.

Управление привилегированным доступом (PAM)
Решения PAM работают за счет предоставления доступа к системам только тогда, когда это необходимо, по указанным причинам и в течение ограниченного периода времени; а зрелые решения предлагают такие функции, как мониторинг сеансов для целей расследования и аудита, или автоматические службы управления паролями / ротации для предотвращения "распыления паролей". Чтобы развернуть и использовать PAM, необходимо понять, кто из сотрудников имеет доступ к различным системам. Предоставление доступа к данным или системам только в случае необходимости представляет собой "Принцип наименьших привилегий" (PoLP). Перед развертыванием любых решений Aon рекомендует сначала проанализировать текущих пользователей и права доступа в организации и определить политику управления доступом, необходимую для реализации технологического плана - определить, кто и когда должен иметь доступ, и как это будет контролироваться. После введения политики компания Aon рекомендует развернуть решение PAM для управления доступом администраторов и постоянного контроля и аудита этой политики. В Великобритании Национальный центр кибер-безопасности (NCSC) рекомендует использовать решение по управлению привилегированным доступом, "устраняющее необходимость прямого доступа администраторов к дорогостоящим системам резервного копирования" и минимизирующее этот риск .[5]

Многофакторная аутентификация (MFA)
Многие стратегии цифровой трансформации увеличивают количество и тип бизнес-систем, предоставляемых бизнес-пользователям, что означает необходимость множественной аутентификации. Точки аутентификации предоставляют возможность для компрометации злоумышленниками, использующими методы "распыления пароля", "грубой силы" или "набивки учетных данных". Контроль, который может помочь снизить этот риск, — это многофакторная аутентификация (MFA), которая представляет собой способ аутентификации пользователей, требующий более двух форм аутентификации для получения доступа к системе с примерами дополнительных шагов проверки, включая биометрические данные, SMS-верификацию и секретные вопросы / ответы. Добавляя дополнительный уровень проверки, предприятия могут снизить вероятность - или легкость - методов компрометации учетных записей, которые могут быть первым этапом угрозы со стороны злоумышленников.

5. https://www.ncsc.gov.uk/collection/secure-system-administration/use-privileged-access-management

При рассмотрении MFA Aon рекомендует сначала проанализировать цели для конкретного бизнес-объекта и определить критерии успеха, критические группы пользователей, критические активы, количество пользователей и общий процесс управления. После определения целей и процессов следует рассмотреть вопрос о развертывании или принятии соответствующего инструментария, который будет зависеть от бизнес-системы и существующих технологий. Организациям следует рассмотреть доступные варианты развертывания (облачно или стационарно), типы функциональности и интеграцию с другими ключевыми функциями (например, PAM или требования к центру управления безопасностью). Национальный центр кибер-безопасности Великобритании заявляет, что "должна быть включена многофакторная аутентификация (MFA), и метод MFA не должен устанавливаться на том же устройстве, которое используется для администрирования резервных копий".[6]

Обучение и осведомленность

Злоумышленники часто стремятся использовать ничего не подозревающих бизнес-пользователей для проведения атаки. Во время сбоев в работе организации злоумышленники стремятся воспользоваться преимуществами ничего не подозревающих бизнес-пользователей, проводя разведку. Обучение персонала методам защиты от атак становится критически важным аспектом. Отсутствие знаний почти никогда не является виной пользователя, но должно решаться организацией в форме структурированной кампании по обучению и повышению осведомленности для предоставления конечным пользователям знаний и обучения их навыкам, необходимым для обеспечения личной и деловой безопасности.

Симуляция фишинга

Одним из способов выявления пробелов в осведомленности сотрудников безопасности является симуляция фишинга. Одним из наиболее распространенных методов атаки являются фишинговые письма, призванные обманом заставить людей передать конфиденциальную информацию, которая может быть использована для доступа к защищенным данным, сетям и системам. ***Только в первые недели пандемии COVID-19 число попыток фишинга возросло более чем на 600%.***[7] Фишинговая атака может привести к критическим последствиям для бизнеса, поэтому очень важно, чтобы организации помогли сотрудникам понять, что такое фишинг и как обнаружить и сообщить о попытках его совершения. Хорошо спланированная кампания имитирует реальные фишинговые атаки, чтобы оценить осведомленность сотрудников о безопасности, выявить пробелы в знаниях и улучшить процессы обучения пользователей, чтобы помочь распознать угрозы, которые могут представлять такие атаки.

Готовность к реагированию на инциденты

В случае кибер-инцидента быстрое обнаружение и реагирование могут иметь решающее значение для минимизации последствий. Жизненно важно подготовить организацию к реагированию на кибер-инциденты, такие, как атака программ-вымогателей среди людей, процессов и технологий. Данный процесс включает в себя основные возможности, описанные ниже, для разработки и тестирования планов и функций реагирования на инциденты.

План реагирования на инциденты

Первым аспектом, с которого следует начинать подготовку к реагированию на инциденты, является план. Комплексный план, который регулярно проходит стресс-тестирование, помогает гарантировать, что предприятие сможет задействовать нужные ресурсы в нужное время на протяжении всего жизненного цикла инцидента, обеспечивая упорядоченность всех процессов. В нем должны быть описаны основные шаги, которые необходимо предпринять в случае инцидента (организации обычно опираются на NIST Incident Response Framework: подготовка, обнаружение и анализ, локализация, ликвидация и восстановление), а также он должен быть согласован с более широкой политикой безопасности и кризисного управления. Ключевым фактором является предварительное согласование ролей и ответственности в случае наступления кибер-инцидента; необходимо рассмотреть юридические вопросы, PR, HR, IT, C-Suite и т.д., и установить, кто и за что несет ответственность. Для каждой фазы процесса реагирования на риск следует определить четкие линии связи, управления и эскалации, а также продумать план действий для определения воздействия на бизнес и соответствующие меры предотвращения, сдерживания и восстановления, которым необходимо следовать в случае возникновения инцидента. Следует также рассмотреть вопрос порядка получения доступа к этому плану, кто должен иметь доступ и как регулярно стоит его проверять.

Тестирование плана реагирования на инциденты

Чтобы оценить полноту возможностей плана реагирования на инциденты во время потенциального события, связанного с вымогательским ПО, компания Aon предлагает провести целевые учения по моделированию кибер-угроз. Тестирование плана реагирования на инциденты должно проводиться как на техническом уровне, так и на уровне руководства для оценки уместности, полноты и эффективности имеющихся средств контроля для смягчения последствий и управления реакцией на атаки. Тестирование должно включать тщательную проработку сценариев, соответствовать реалистичным сценариям и быть адаптировано к рискам, с которыми сталкивается организация. Организациям следует фиксировать полученные уроки, чтобы выявить основные сильные стороны, недостатки, риски и рекомендации по улучшения плана.

6 . https://www .ncsc .gov .uk/guidance/multi-factor-authentication-online-services

7. https://www.accenture.com/us-en/blogs/business-functions-blog/the-human-aspect-of-cyber-security-in-a-covid-19-world

Обнаружение

Выявление и обнаружение событий и инцидентов кибер-безопасности до начала реагирования

Меры контроля, которые необходимо рассмотреть:

Применяется ли постоянное сканирование уязвимостей сети?

Используете ли вы упреждающие сведения об угрозах для отслеживания тактики, методов и процедур (TTP) кибер-злоумышленников?

Функция *обнаружения* рассматривает разработку средств контроля и мер, позволяющих выявлять и обнаруживать события и инциденты кибер-безопасности до инициации процесса реагирования. Помимо развертывания программного обеспечения, выполняющего антивирусное сканирование (что следует считать негласным требованием), многие организации инвестируют в возможности защитного мониторинга для обеспечения видимости всей системы. Возможности обнаружения, такие, как операционный центр безопасности (SOC), мониторинг событий информационной безопасности (SIEM) или обнаружение и реагирование на конечные точки (EDR), могут стать важнейшими инструментами для поиска и обработки событий / инцидентов безопасности и должны использовать основанный на оценке рисков подход к применяемым правилам обнаружения.

Многие из этих возможностей могут обеспечивать как обнаружение, так и реагирование (см. EDR). Aon рекомендует создать инструментарий и процессы, необходимые для проактивного обеспечения видимости событий во всем технологическом комплексе с помощью защитного мониторинга безопасности и использования таких возможностей, как анализ угроз для обнаружения внешних угроз и опережения кибер-инцидентов до их возникновения.

Мониторинг уязвимостей

Одним из ключевых элементов на этапе обнаружения является способность обнаруживать известные уязвимости и вредоносный код в целевой среде. Чтобы найти и устранить уязвимости до того, как они станут инцидентами, Aon рекомендует использовать постоянное сканирование уязвимостей сети. Для критически важных систем или систем, подключенных к Интернету, возможность непрерывного анализа уязвимостей может обратить внимание на те, которые возникают в результате обновления конфигурации и системы управления. Организациям следует тщательно изучить инструментарий и услуги, способные обеспечить это, при этом, важнейшим результатом является отчетность.

Цель - предоставить ИТ-команде инструменты, необходимые для выявления уязвимостей в сетевой инфраструктуре, приложениях и API (в Интернете или внутри компании), а затем отслеживать и управлять устранением выявленных проблем до того, как ими сможет воспользоваться злоумышленник.

Используйте аналитику угроз, чтобы оставаться впереди

В дополнение к возможностям защитного мониторинга на уровне сети, использование анализа угроз может иметь решающее значение для проактивного выявления угроз (внутренних и внешних) в дополнение к скомпрометированным учетным данным, субъектам угроз и пр. Решения безопасности на основе инструментария обеспечивают прочную основу для обнаружения событий безопасности в реальном времени и могут быть дополнены использованием проактивной разведки угроз, которая отслеживает тактику, методы и процедуры (TTP) противников, которые могут быть использованы для защиты от конкретных стратегий.

Aon рекомендует рассмотреть профиль угроз организации и разработать ряд ключевых критериев поиска для определения направленности функции анализа угроз. Развитая функция разведки угроз должна обладать способностью осуществлять мониторинг в различных отраслях, географических регионах, на различных языках и в различных источниках информации (например, deep / dark web, хакерские форумы и т.д.) и сопоставлять информацию для определения вероятности и степени угроз, с которыми сталкивается организация.

Как правило, разведка угроз может проводиться либо как разовое мероприятие (например, с фокусом на конкретной угрозе или событии), либо как постоянная возможность поддержки функции информационной безопасности. Aon рекомендует использовать постоянную функцию проактивной разведки угроз на основе ключевых угроз и оценивать их непосредственно в периоды изменения бизнеса или технологий.

Реагирование

Принятие мер реагирования в случае инцидента с вымогательским ПО.

Меры контроля, которые необходимо рассмотреть:

Используете ли вы обнаружение и реагирование на конечных точках (EDR) в качестве средства кибер-защиты?

Функцияя *реагирования* учитывает важность принятия соответствующих мер для эффективного реагирования в случае крупного кибер-инцидента. Как указано в других частях данных рекомендаций, планирование и отработка планов реагирования на инциденты являются ключевыми, равно как и в сценарии реагирования, когда в распоряжении организации есть правильные инструменты, которые могут иметь решающее значение при управлении воздействиями.

Жизненный цикл реагирования на кибер-инциденты NIST включает в себя четыре ключевых этапа:

- **Подготовка**
- **Обнаружение и анализ**
- **Сдерживание, уничтожение и восстановление**
- **Деятельность после инцидента**

Наличие и регулярное тестирование специально разработанного плана реагирования на инциденты является важнейшим фактором способности организации реагировать на кибер-инциденты в случае их возникновения. Благодаря проактивному реагированию с помощью функций обнаружения, сканирования и анализа угроз, можно отлавливать события на более ранних этапах цепочки поражения, чтобы предотвратить и минимизировать последствия. В дополнение к этим факторам, Aon рекомендует использовать соответствующие инструменты, способные сдерживать, уничтожать угрозу и восстанавливать работу в режиме реального времени таким образом, чтобы организации могли уменьшить распространение, масштаб и воздействие инцидента.

Использование EDR для локализации, анализа, смягчения последствий и улучшения ситуации в режиме реального времени

Как и во многих других атаках на кибер-безопасность, исходной точкой входа для злоумышленников часто является фишинг или целевой фишинг через открытие зараженного вложения электронной почты или нарушение настройки оборудования для удаленного доступа. Многие угрозы, связанные с выкупом, могут заражать оборудование и сети и обходить традиционные средства защиты, такие как антивирусы (AV).

Учитывая, что первоначально зараженное целевое устройство или "конечная точка" является первой точкой входа злоумышленников в корпоративную сеть, одним из наиболее важных инструментов кибер-защиты является платформа Endpoint Protection Platform (EPP) и, в частности, Endpoint Detection & Response (EDR). Современные возможности EDR обеспечивают организациям видимость (см. раздел "Обнаружение") атак, происходящих на устройствах (конечных точках) во всей их технологической инфраструктуре, чтобы обеспечить контекст и контроль устранения последствий, необходимые для реагирования на инциденты в реальном времени. Благодаря созданию развитой системы EDR в рамках операции кибер-защиты организаций, появляется возможность проактивно сдерживать угрозы и реагировать на них в режиме реального времени после того, как произошло первоначальное вредоносное вмешательство.

Aon рекомендует использовать функцию EDR, которая может применять методы анализа угроз и моделирования данных для анализа активности в реальном времени, чтобы проактивно изолировать активность, распознанную или указывающую на угрозу вымогателя до того, как трафик расширится в другом месте. Передовые возможности EDR дополняют это возможностью изолировать, исследовать и реагировать на подозрительные файлы и программное обеспечение, которое может предоставить дополнительную важную информацию, чтобы опередить злоумышленников и проактивно обновить остальные элементы управления защитой конечных точек организации в режиме реального времени.

Создание возможностей реагирования с использованием EDR - это нечто большее, чем просто развертывание инструмента, и требует сочетания процесса, управления и инструментария, которые сначала необходимо создать для эффективной работы. Как только требования и модель поддержки становятся понятны, Aon рекомендует инвестировать в соответствующие инструменты EDR, которые могут быть развернуты на всей территории, используя разведку угроз и технологии для анализа индикаторов компрометации (IOCs) и индикаторов поведения (IOBs) в режиме реального времени для проактивной блокировки угроз, которые традиционные антивирусные средства могли пропустить.

Восстановление

Восстановление бизнес-операций и минимизация последствий инцидента с участием программ-вымогателей.

Меры контроля, которые необходимо рассмотреть:

Учитывают ли ваши планы обеспечения непрерывности деловой активности и аварийного восстановления (BCDR) угрозы , исходящие от вымогательского ПО и регулярно ли они проверяются?

Риски, исходящие от программ-вымогателей, **постоянно меняются и развиваются,** и чтобы управлять ими должным образом, требуется комбинированная стратегия не просто кибер-безопасности, рисков и страхования, но и мер контроля, изложенных в данных рекомендациях.

.

Функция *восстановления* сосредоточена на возможности восстановления организации после инцидента, а также на готовности к возобновлению деловой активности. Это достигается путем разработки и использования проверенных и испытанных планов для минимизации последствий кибер-атак, таких как простои, перерывы в производстве и/или потери в производительности. В этом разделе рекомендаций конкретно рассматривается необходимость участия в планировании обеспечения непрерывности деловой активности, которое согласовано с планами / сценариями реагирования на инциденты, связанные с программами-вымогателями, и регулярно тестируется в рамках деловой активности.

Планирование непрерывности деловой активности и аварийного восстановления (BCDR)

В соответствии с планом реагирования, необходимо разработать специальный план BCDR, учитывающий риски / потери от кибер-атаки. Планирование непрерывности деловой активности является обычным делом на большинстве предприятий, однако многие организации не адаптировали существующую практику для отражения развития организации и не являются достаточно динамичными для отражения меняющейся среды риска, что включает в себя планирование BCDR, например, обеспечение регулярного резервного копирования и надлежащей защиты.

Aon рекомендует готовиться к инциденту, разрабатывая планы BCDR, связанные с процессами реагирования на инциденты, а затем тестируя и обновляя эти планы в ходе итерационного процесса. Это поможет обеспечить постоянное совершенствование подхода к BCDR в отношении вымогательского ПО, а также предоставит организациям следующие возможности совершенствования через "извлеченные уроки".

ФАЗА 1	ФАЗА 2	ФАЗА 3
Анализ текущего ландшафта рисков, связанных с программами-вымогателями (*см. раздел "Обнаружение"*): распознать основные сценарии программ-вымогателей, которые могут повлиять на организацию, и рассмотреть потенциальные последствия, требующие разработки плана BCDR.	**Обзор существующей стратегии BCDR:** проанализировать существующую стратегию BCDR организации, чтобы убедиться, что конкретные сценарии вымогателей согласованы соответствующим образом.	**Согласование планов BCDR со сценариями воздействия программ-вымогателей:** разработка и согласование конкретных планов BCDR для организации, которые могут быть использованы при столкновении с вымогательским ПО.

Как и в случае с каждой из рекомендаций, изложенных в данном документе, ни один из видов контроля не может обеспечить всеобъемлющую обороноспособность, равно как и сила одного из них не компенсирует силу другого. Внедрение и постоянное тестирование эффективности этих средств контроля крайне важно, учитывая, что злоумышленники постоянно совершенствуют свои методы атак, а сами атаки становятся все более частыми, целенаправленными, изощренными и дорогостоящими.

Каков уровень зрелости защиты вашей организации от программ-вымогатлей?

Понимание сильных и слабых сторон, а также областей совершенствования, является важнейшим первым шагом на пути к обеспечению готовности к защите от атак. Организации могут получить первоначальное представление о степени зрелости, заполнив контрольный список Aon по защите от вымогательского ПО.

Какова степень зрелости защиты вашей организации от вымогательского ПО?

Заполните контрольный список и обратитесь к расшифровке результатов, приведенной ниже, чтобы определить общий уровень зрелости защиты вашей организации.

Уровень зрелости защиты организации от вымогательского ПО	Значение
Начальная готовность	10 -14
Базовая готовность	15-24
Установлен управляемый контроль	25-34
Усовершенствованные средства контроля	35+

Контрольный список Aon по защите от программ-вымогателей отражает наши рекомендуемые методы и может помочь быстро и просто определить уровень зрелости и готовности вашей организации. Эта информация может обеспечить первоначальную критическую видимость готовности к атакам и определить приоритеты улучшений и инвестиций, необходимых для обеспечения безопасности.

Шаги по заполнению чек-листа

Шаг 1

Для начала необходимо проработать 10 вопросов по управлению защитой от программ-вымогателей

Шаг 2

Присвойте себе оценку зрелости и запишите ее в соответствующем поле на сетке. Например, если вы набрали «Начальный уровень» по вопросу 1, укажите цифру 1 в соответствующем поле.

Шаг 3

После завершения сложите общий балл для каждой из пяти областей управления защитой от программ-вымогателей (идентификация, защита, обнаружение, реагирование и восстановление).

Шаг 4

В заключение сложите свои общие баллы для каждой области управления защитой от программ-вымогателей, чтобы определить окончательное значение баллов и указать общий балл вашей организации.

> Aon способствует пониманию текущей степени зрелости вашей системы для определения приоритетов по усовершенствованию и обсуждения дальнейших шагов

Контрольный список Aon по защите от вымогательского ПО

Контроль защиты от вымогательского ПО	Оценка зрелости				Оценка
	Начальная готовность = 1 В данный момент контроль над вредоносным ПО не осуществляется или не существует	**Базовая готовность = 2** Контроль над вредоносным ПО осуществляется на разовой основе или неформализованным образом	**Управляемый контроль = 3** Контроль над вредоносным ПО установлен в большинстве организаций	**Усовершенствованные средства контроля = 4** Общеорганизационный подход к управлению над вымогательскими программами	
Определение Понимаете ли вы профиль атаки вашей организации и проанализировали ли вы управление, контроль, роли и обязанности?					
Проверили ли вы свой уровень защиты, проанализировав средства контроля безопасности ключевых систем?					
Защита Развернули ли вы систему управления доступом к привилегиям (PAM)?					
Применены ли средства многофакторной аутентификации (MFA)?					
Постоянно ли вы повышаете осведомленность сотрудников о кибер-безопасности, например, с помощью симуляторов фишинга?					
Имеется ли у вас адекватный план реагирования на инциденты, и как давно он проверялся?					
Обнаружение Применяется ли постоянное сканирование уязвимостей сети?					
Используете ли вы упреждающие сведения об угрозах для отслеживания тактики, методов и процедур (TTP) кибер-злоумышленников?					
Реагирование Используете ли вы обнаружение и реагирование на конечные точки (EDR) в качестве средства кибер-защиты?					
Восстановление Учитываются ли в ваших планах обеспечения непрерывности деловой активности и аварийного восстановления (BCDR) кибер-угрозы и программы-вымогатели и проводятся ли регулярные проверки на них?					
			Всего		

Чтобы помочь с постоянным повышением уровня зрелости защиты от программ-вымогателей, компания Aon разработала **Комплект Защиты от Программ-вымогателей**, предназначенный для снижения уязвимостей и усиления контроля. **Чтобы узнать больше, свяжитесь с локальным представителем Aon**.

Контакты

За дополнительной информацией обращайтесь к нашим консультантам по кибер-безопасности в регионе EMEA:

Крайг Ратланд
Вице-президент по кибер-безопасности в регионе EMEA
+44 (0)7557 578 737
kraig .rutland@aon .co .uk

Джон Тейлор-Гой
Вице-президент по развитию бизнеса в регионе EMEA Cyber Security
+44 (0)7881 848811
jon .taylor-goy@aon .co .uk

Энди Кэтли
Директор по кибер-безопасности в регионе EMEA
+44 (0)7824 547 805
andy .catley@aon .co .uk

Посетите сайт aon.com/cyber-solutions

Об Aon

Aon plc (NYSE:AON) - ведущая мировая компания по оказанию профессиональных услуг, предоставляющая широкий спектр решений в области рисков, пенсионного обеспечения и здравоохранения. 50 000 сотрудников в более чем 120 странах мира позволяют добиться результатов для клиентов, используя запатентованные данные и аналитику для получения информации, позволяющей снизить волатильность и повысить эффективность работы.

Услуги в области кибер-безопасности, предлагаемые компанией Stroz Friedberg Inc. и ее аффилированными лицами.

Услуги в области кибер-рисков в регионе EMEA и Великобритании предоставляются компанией Aon UK Limited и ее аффилированными лицами.

Aon UK Limited уполномочена и регулируется Управлением по финансовому регулированию и надзору (FCA) в отношении деятельности по распространению страховых услуг.

Следующие продукты или услуги не регулируются FCA:

- Услуги в области кибер-рисков, предоставляемые компанией Aon UK Limited
- Услуги по кибер-безопасности, предоставляемые компанией Stroz Friedberg Limited и ее аффилированными лицами

Данная информация приведена лишь в ознакомительных целях и не предназначена для предоставления консультаций. По вопросам страхового покрытия или специфических рисков всегда следует обращаться за профессиональной консультацией.

Несмотря на то, что при подготовке данной статьи были приняты все меры предосторожности, компания Aon UK Limited не гарантирует полноту или пригодность для какой-либо цели данной статьи или любой ее части и не несет ответственности за любые убытки, понесенные каким-либо образом любым лицом, которое может полагаться на нее. При любых обстоятельтсвах любой получатель несет полную ответственность за использование данной статьи.