Кибер-решения Aon

Комплекс мер по защите от программ-вымогателей

Индивидуальный набор услуг по обеспечению кибер-безопасности, помогающий организациям смягчить последствия атаки программ-вымогателей.

"Инциденты с использованием программ-вымогателей становятся все более **частыми, изощренными и целенаправленными,** а размеры выкупа растут. В результате такой динамики многие предприятия становятся более уязвимыми к кибер-угрозам и **не могут обеспечить необходимое страховое покрытие, которое им требуется** в ответ на событие. **Проактивная защита от программ-вымогателей** предоставляет клиентам комплексное решение в свете этих проблем".

Ричард Хэнлон, коммерческий директор по региону EMEA, Aon's Cyber Solutions

Программы-вымогатели быстро становятся **доминирующим инструментом для кибер-преступников**, намеревающихся извлечь из своих жертв максимальную выгоду, используя двойную угрозу: **парализацию бизнес-систем** и использование похищенных конфиденциальных данных для получения выкупа[1].

Атаки программ-вымогателей становятся все более частыми, целенаправленными, изощренными и дорогостоящими. Программы-вымогатели представляют собой риск, который нельзя недооценивать, поскольку они могут нанести значительный финансовый и репутационный ущерб. Методы, используемые злоумышленниками, не стоят на месте, равно как и не должны стоять на месте средства защиты, которые организации используют для нейтрализации вредоносных действий.

Понимание проблем

- Мы понимаем важность ключевых элементов управления, проблемы, связанные с их разработкой, и время, необходимое для реагирования на действия злоумышленников и восстановления работоспособности бизнеса.

- Комплекс мер защиты от программ-вымогателей Aon сочетает в себе опыт, полученный при реагировании на инциденты из первых рук, и предоставление кибер-решений для ряда самых сложных бизнес-сред по всему миру.

- Наши широкие возможности по консультированию в области безопасности, тестированию, расследованиям и реагированию, рискам и страхованию обеспечивают перекрестную перспективу в отношении того, какие элементы управления имеют значение и как их можно оптимизировать для защиты от программ-вымогателей. Такой подход также может способствовать принятию решений о страховании, демонстрируя готовность организации.

[1] Источник: Aon's Cyber Security Risk Report 2021

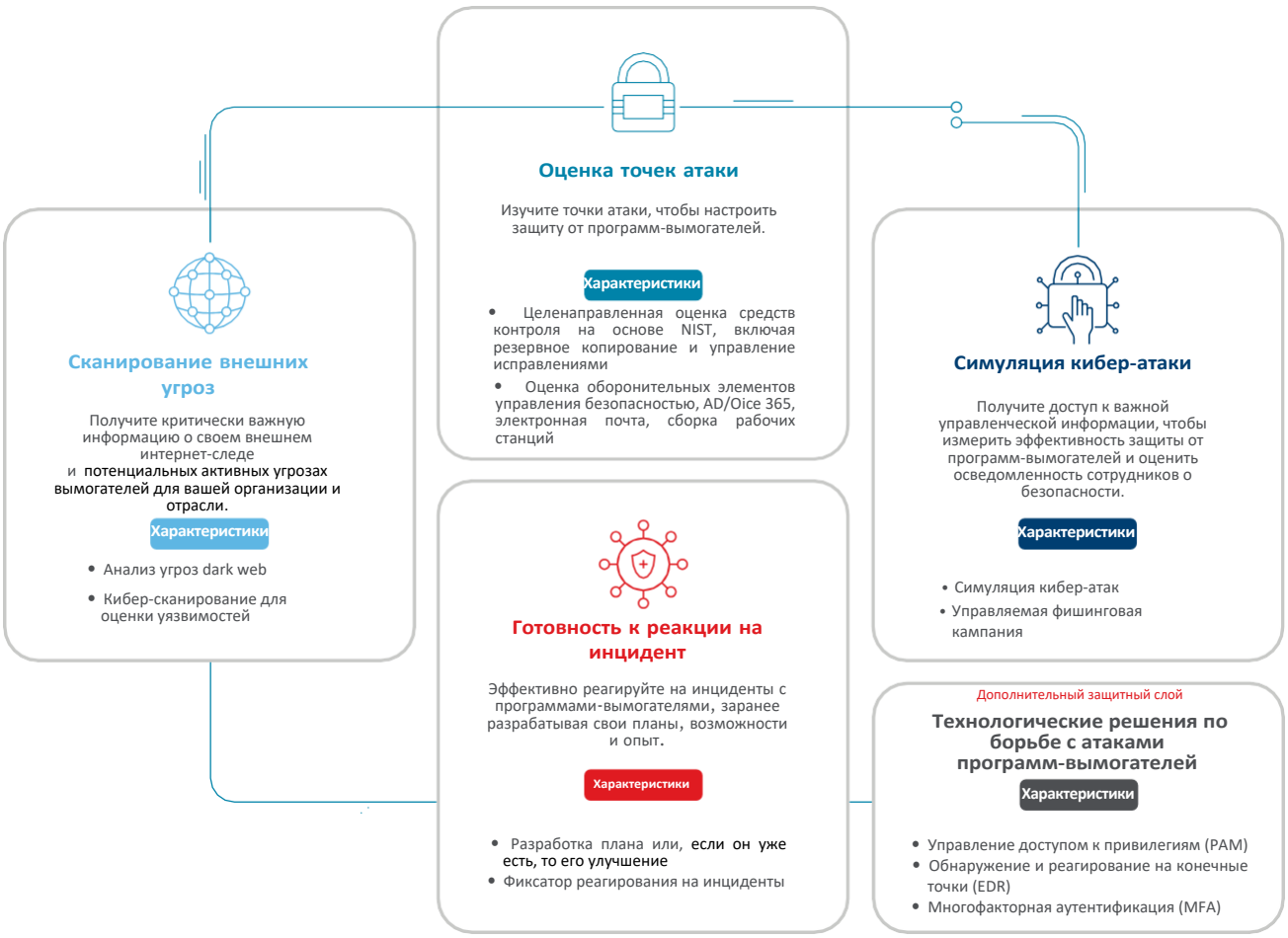
Как Aon может помочь

- Комплекс мер Aon **объединяет данные и отраслевую аналитику, собранную более чем за 20 лет,** а также наш опыт в реализации целевых стратегий защиты от программ-вымогателей в четырех ключевых областях:

- **Оценка точек атаки:** Определите точки атаки, чтобы настроить защиту от программ-вымогателей.
- **Сканирование внешних угроз:** Получите критически важную информацию о своем внешнем интернет-следе и потенциальных активных угрозах вымогателей для вашей организации и отрасли.
- **Симуляция кибер-атаки:** Получите доступ к важной управленческой информации, необходимой для измерения эффективности защиты от программ-вымогателей, а также для оценки осведомленности сотрудников о безопасности.
- **Готовность к реагированию на инциденты:** Эффективно реагируйте на инциденты, связанные с вымогательским ПО, заранее разрабатывая свои планы, возможности и опыт.

Комплекс мер защиты Aon от программ-вымогателей

Специально подобранный набор услуг по обеспечению кибер-безопасности, которые помогают организациям предотвращать и смягчать последствия атаки программ-вымогателей и лучше поддерживать решения о страховании, демонстрируя тщательную и усердную готовность.



Оценка точек атаки

Как мы можем помочь

Программа Aon's Attack Surface Assessment использует коллективные возможности кибер-решений Aon для анализа средств предотвращения, обнаружения, реагирования и восстановления организации, чтобы понять, насколько эффективно они могут защитить организацию от вредоносного ПО или смягчить его последствия.

Оценивая технические и технологические средства контроля безопасности, мы помогаем организациям получить представление об охвате и глубине возможностей, необходимых для управления угрозами, а также предоставляем экспертные рекомендации по устранению последствий.

При оформлении полиса кибер-страхования страховщики проверяют...

☑ **...была ли проведена самооценка в отношении средств предотвращения, обнаружения,** реагирования и восстановления.

Сканирование внешних угроз

Как мы можем помочь

CyberScan от Aon позволяет организации постоянно отслеживать активы, выходящие в интернет, и понимать уязвимости, которые могут быть использованы злоумышленниками в рамках атаки.

Это дополняется предоставлением целевой информации об угрозах, которая может выявить потенциальное нарушение, которое могло произойти или происходит в настоящее время. Эта мощная возможность позволяет организациям подготовиться к принятию соответствующих мер по борьбе с программами-вымогателями.

☑ **...была ли проведена должная проверка, чтобы показать, что у организаций есть возможность обнаружить вторжение и** быстро и эффективно справиться с ним.

Моделирование кибер-атак

Как мы можем помочь

Имитация кибер-атаки от Aon - это совместное упражнение, которое позволяет организациям понять, насколько их процессы обнаружения и/или возможности предотвращения подходят для противодействия атакам программ-вымогателей.

Наша служба управляемого фишинга имитирует фишинговые атаки в реальном времени, используемые злоумышленниками-вымогателями, для оценки осведомленности сотрудников о безопасности, выявления пробелов в их знаниях и обучения пользователей способам распознавания угроз, которые могут представлять эти атаки.

☑ ...**был ли установлен интернет-след,** по которому можно определить потенциальные векторы атак, которыми могут воспользоваться злоумышленники.

Готовность к реагированию на инциденты

Как мы можем помочь

Планы реагирования на инциденты разрабатываются с учетом меняющихся требований наших клиентов, в результате чего планы получаются надежными и соответствующими своему назначению с высоким уровнем положительных отзывов.

Планшетные учения помогают организациям в проверке эффективности планов реагирования на инциденты.

Фиксаторы планов - задействуются в случае атаки программ-вымогателей - предоставление доступа к глобальному круглосуточному и 365-дневному центру планирования реагирования на инциденты Aon и нашей команде цифровой криминалистики для оказания помощи в сортировке, анализе, локализации и восстановлении организационных активов.

При оформлении полиса кибер-страхования страховщики проверяют...

☑ **...имеется ли план реагирования для людей, процессов и технологий** в случае кибер-инцидента.

Технологические решения для борьбы с вымогательством

Дополнительный защитный слой

Как мы можем помочь

Управление доступом к привилегиям (PAM): Эти решения работают путем предоставления доступа к системам только при необходимости, по указанным причинам и на ограниченное время - вместо предоставления постоянного расширенного доступа к системе, который может быть использован в дальнейшем.

Обнаружение и реагирование на конечные точки (EDR):

Для критически важных систем или систем, подключенных к Интернету, возможность постоянного анализа на наличие уязвимостей может обеспечить немедленное внимание к тем из них, которые возникают в результате обновления конфигурации или системы управления.

Многофакторная аутентификация (MFA): Существует несколько типов MFA, и выбор подходящего зависит от конкретного бизнеса и существующих технологий - примерами дополнительных шагов проверки могут быть биометрия, SMS-верификация, секретные вопросы / ответы и другие.

Наш подход

- Пакет по борьбе с атаками программ-вымогателей дает организациям возможность лучше понимать, смягчать и управлять текущими и возникающими рисками, с которыми они сталкиваются.
- В связи с постоянно меняющимся характером атак и методов, организациям часто трудно определить возможности, необходимые для обеспечения безопасности. Это было недавно подчеркнуто в отчете Aon "Кибер-безопасность 2021", где ***только 31% организаций из всех отраслей считают, что у них имеются адекватные меры по повышению устойчивости бизнеса для борьбы с вымогательским ПО***.
- Готовность к атаке программ-вымогателей требует продуманного подхода, использующего соответствующие средства управления людьми, процессами и технологиями, контроль за которыми может быть сложным и дорогостоящим.

Основные преимущества

- **Систематическая оценка и выявление рисков программ-вымогателей** и оптимизация средств защиты от программ-вымогателей
- **Снижение вероятности проникновения в сеть** в результате атак программ-вымогателей
- **Обеспечение постоянного управления уязвимостями и видимости** потенциальных угроз **с помощью сканирования Dark Web.**
- **Повышение осведомленности сотрудников о кибер-безопасности** через имитацию фишинга
- **Проверка готовности к реагированию на инциденты**

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.

© Aon plc 2021. Все права защищены.

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.

FP.AGRC.436.AP

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. В любом случае любой получатель несет полную ответственность за использование данной статьи.