Международная организация гражданской авиации

A41-WP/241
EX/108
2/8/22

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 41-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 14 повестки дня. Авиационная безопасность. Политика

ОБЕСПЕЧЕНИЕ АВИАЦИОННОЙ БЕЗОПАСНОСТИ В СООТВЕТСТВИИ С КОНЦЕПЦИЕЙ НУЛЕВОГО ДОВЕРИЯ

(Представлено Южно-Африканской Республикой)

КРАТКАЯ СПРАВКА

Авиационная отрасль до некоторой степени зависит от длинных цепочек поставок, проходящих через другие отрасли, что увеличивает количество рисков для авиации. Внедрение систем на основе протокола Интернет (IP) для повышения эффективности требует принятия упреждающих подходов к защите современных и традиционных систем.

В Плане действий ИКАО по обеспечению кибербезопасности подчеркивается необходимость сконцентрировать ресурсы и действия на выработке системного подхода к управлению кибербезопасностью в авиации с целью создать подход по принципу "системы систем", который позволяет авиации своевременно адаптироваться и противостоять новым угрозам.

В настоящем рабочем документе делается попытка изложить концепцию нулевого доверия, которую государства и другие участники авиационной отрасли могли бы принять в качестве одного из принципов уменьшения подверженности рискам. Внедрение концепции нулевого доверия способно укрепить текущие возможности в сфере кибербезопасности за счет обеспечения сквозной защиты систем. Это отличается от традиционной защиты периметра тем, что ресурсы безопасности используются на периферии или ближе к оборудованию управления трафиком конечных пользователей и к данным, предоставляемым наземными навигационными средствами в отдаленных районах (от радиолокаторов).

Действия: Ассамблее предлагается:

a) признать преимущества внедрения гибких и адаптивных подходов непрерывной адаптивной оценки рисков и доверия (CARTA) в обеспечении защиты авиационной деятельности;

b) поручить ИКАО через Группу экспертов по кибербезопасности разработать технический инструктивный материал, который помог бы государствам включить концепцию нулевого доверия в системы управления информационной безопасностью (СУИБ);

c) призвать государства рассмотреть возможность включения принципов нулевого доверия в свои СУИБ.

Стратегические цели	Данный рабочий документ связан со стратегической целью *"Авиационная безопасность и упрощение формальностей"*

Финансовые последствия	Дополнительные последствия для бюджета отсутствуют, поскольку работа будет проводиться в рамках бюджета, выделенного ИКАО
Справочный материал	*План действий по обеспечению кибербезопасности* Doc 8973, *Руководство ИКАО по авиационной безопасности*

1. ВВЕДЕНИЕ

1.1 В последние годы в авиационной отрасли произошли изменения, вызванные внедрением технологий и, как следствие, увеличением киберрисков, требующих особого внимания. Беспрецедентный гигантский скачок в плане внедрения технологий требует постоянного внедрения подходов и моделей непрерывной адаптивной оценки рисков и доверия (CARTA).

1.2 В предыдущие годы авиационная отрасль рассматривалась самостоятельно. Однако взаимозависимость и конвергенция информационных технологий (ИТ) и операционных технологий (ОТ) в авиационной экосистеме привели к появлению различных заинтересованных сторон, к которым неприменимы механизмы регулирования соответствия нормам авиации. В связи с этим увеличилась возможная область кибернападений, и требуется пересмотр некоторых традиционных концепций.

1.3 Ранее управление авиационным оборудованием и программным обеспечением и его техническое обслуживание можно было осуществлять с помощью защищенной доверенной виртуальной частной сети с удаленным доступом, однако в современном мире такие соединения ставят безопасность систем под угрозу.

1.4 Киберугрозы, такие как программы-вымогатели, кража данных и фишинговые атаки, стали широко распространены в авиационной отрасли, что влияет на среды ИТ (доступ к ERP, услуги совместной работы, услуги электронной почты) и ОТ (SCADA, ПЛК), ориентированные на зоны контроля внутри и вокруг аэропортов и дата-центров.

2. ОБСУЖДЕНИЕ

2.1 Длинная цепочка поставок в авиационной отрасли может привести к возникновению киберугроз и, таким образом, повысить потребность в инновационных и новых подходах для соответствующего реагирования на эти угрозы. Это связано с тем, что авиация зависит от множества заинтересованных сторон, использующих разные системы, приложения и технологии, которые необходимо интегрировать друг с другом.

2.2 Важно также отметить, что для осуществления этих операций может потребоваться удаленная поддержка с помощью ресурсов, находящихся как внутри, так и за пределами границ государства, что в еще большей степени делает цепочку создания стоимости воздушных перевозок уязвимой для киберугроз.

2.3 Прежние традиционные методы обеспечения сетевой безопасности, строившиеся на принципе защиты периметра и использовавшиеся для обеспечения необходимой безопасности, доказали свою неэффективность. Об этом свидетельствует увеличение числа киберсобытий в авиации. Как только злоумышленники пересекают периметр, дальнейшее горизонтальное перемещение происходит беспрепятственно.

2.4 Такие концепции, как концепция нулевого доверия, потенциально могут противостоять угрозам следующего поколения и продвинутым угрозам, которые распространены сегодня: каждый запрос, касающийся ресурса, предусматривает запуск процесса оценки состояния безопасности, валидации состояния безопасности и предоставления доступа к ресурсу согласно продуманным и эффективным мерам безопасности.

2.5 Концепция нулевого доверия содержит набор руководящих принципов рабочего процесса, проектирования систем и операций, которые могут использоваться для улучшения состояния безопасности критически важных и конфиденциальных действий с целью недопущения брешей в защите данных и ограничения внутренних горизонтальных перемещений.

2.6 Подход на основе нулевого доверия предполагает, что доверять нельзя никому, ни внутри организации, ни за ее пределами. Этот подход направлен на минимизацию поверхности атаки и основывается на следующих ключевых идеях:

a) периметра не существует: предположение о том, что людям следует доверять, потому что они оказались внутри сети компании, исключается;

b) необходимо обеспечивать верификацию пользователей перед предоставлением доступа и верификацию целостности устройства перед подключением к сети;

c) предположение о том, что пользователи будут делать правильные вещи, исключается, а вместо этого в случае каждого запроса на обслуживание требуется проверка прав доступа;

d) вместо отслеживания недобросовестных действующих субъектов необходимо устанавливать препятствия, которые будут способствовать снижению производительности.

2.7 Внедрение концепции нулевого доверия способно укрепить текущие возможности в сфере кибербезопасности за счет обеспечения сквозной защиты систем. Это отличается от традиционной защиты периметра тем, что ресурсы безопасности используются на периферии или ближе к оборудованию управления трафиком конечных пользователей и к данным, предоставляемым наземными навигационными средствами в отдаленных районах (от радиолокаторов).

2.8 Осуществлению концепции нулевого доверия способствуют различные базовые технологии, обеспечивающие защиту на различных направлениях:

a) микросегментация – одно из наиболее ранних понятий в рамках концепции нулевого доверия, ориентированное в первую очередь на защиту от горизонтального перемещения, чтобы минимизировать эффект брешей. Основной задачей ряда атак является горизонтальное перемещение для получения информации из ключевых сегментов центра обработки и хранения данных. Указанный подход ограничивает несанкционированный обмен данными между сегментами, выполняющими разные рабочие задачи, если у них нет для этого оперативной причины, что минимизирует эффект брешей. В отличие от обеспечиваемой брандмауэрами защиты типа "север–юг", микросегментация направлена на обеспечение безопасности типа "восток–запад" для сегментов, выполняющих разные рабочие задачи;

b) доступ в сети с нулевым доверием предполагает наличие определяемой контекстом логической границы для доступа к приложениям. Цель состоит в том, чтобы минимизировать доступ и злоупотребления за счет организации доступа к приложениям на основе контекста пользователя и контекста устройства. Согласно этой идее, местонахождение сущностного объекта (например внутри сети) не должно автоматически обеспечивать доверие;

c) все приложения в сети скрыты и доступ разрешен на основе таких атрибутов, как идентификатор пользователя, устройство, геолокация и состояние безопасности. Иными словами, пользователи получают доступ к нужным им приложениям, но больше ничего не видят в сети;

d) изоляция удаленного браузера работает по принципу, согласно которому конечные пользователи – это самые слабые звенья в любой организации, а доступ в интернет – одна из крупнейших областей для атаки, в которой возникают бреши. Таким образом, один из наиболее эффективных способов минимизировать компрометацию оконечной точки/конечного пользователя – изолировать доступ в интернет, чтобы исключить эксплуатацию уязвимостей браузеров и избежать таких угроз, как программы-вымогатели, встроенные вредоносные программы и фишинг.

3. ВЫВОД

3.1 Принципы нулевого доверия могут использоваться для самоукрепления гражданской авиации за счет применения подхода встроенной безопасности. Упреждающий подход, предлагающий "встраивание" методов обеспечения безопасности критически важных элементов и процессов, приходит на смену подходу на основе реагирования, предполагающему "надстройку" парадигмы обеспечения безопасности, и способствует развитию самоукрепляющейся системы гражданской авиации, позволяя ей эволюционировать и повышать жизнеспособность в условиях большей автоматизации, что доказало свою эффективность.

— КОНЕЦ —