Приложение 3. Наихудшие сценарии кибератак

написано Александр Астахов | 11 июня, 2023

В следующей таблице приведены наихудшие сценарии кибератак на ключевые элементы инфраструктуры США по отраслям промышленности. Для сравнения наряду с наихудшими сценариями приведены также более реалистичные сценарии, сопровождаемые комментариями специалистов из предметных областей.

№ 1. Отрасль: ЭЛЕКТРИЧЕСТВО

Наихудший, но маловероятный сценарий

Атака на системы управления через беспроводные, модемные или интернет-соединения может послужить причиной временного локального отключения электричества.

Более реалистичный сценарий

Физическое разрушение электростанций или линий связи может привести к отключению электричества на несколько дней.

Комментарий специалиста

«Все электрические компании подключены к Интернет тем или иным способом, однако это не означает, что их системы управления доступны из Интернет».

Элен Ванко, представитель Североамериканского совета по безопасности электроэнергетики

№ 2. Отрасль: ТРАНСПОРТ

Наихудший, но маловероятный сценарий

Атакующий может через Интернет подключиться к одной из 500 систем управления железными дорогами и вызвать столкновение электропоездов, направив их на один путь.

Более реалистичный сценарий

Использование на поездах горючего, содержащего опасные вещества, может привести к отравлению окружающей среды.

Комментарий специалиста

«Мы знаем, что имеются возможности для нанесения ущерба, и стараемся ликвидировать все известные дыры в защите наших систем. Рассматриваем ли мы кибертерроризм в качестве более серьезной угрозы, нежели обычный физический терроризм? Однозначно – нет».

Нэнси Вильсон, старший ассистент вице президента Ассоциации американских железных дорог

№ 3. Отрасль: ВОДНЫЕ РЕСУРСЫ

Наихудший, но маловероятный сценарий

Вода может быть заражена путем повышения содержания хлора или других химических веществ в результате осуществления атаки на систему управления через Интернет, по коммутируемому или беспроводному соединению.

Более реалистичный сценарий

Химические или биологические отравляющие вещества могут быть добавлены в воду физически. Однако многочисленные проверки химического состава воды сводят этот риск к минимуму.

Комментарий специалиста

«Большую часть денег, выделенных на обеспечение безопасности водных предприятий, стоило бы потратить на их физическую защиту».

Дайан Ван Де Хей, исполнительный директор Ассоциации столичных водных агентств

№ 4. Отрасль: ЭНЕРГЕТИКА

Наихудший, но маловероятный сценарий

Вывод из строя частей Интернет, используемых системами торговли нефтью, может остановить покупки и продажи и привести к временному отключению источников энергии.

Более реалистичный сценарий

Физическое разрушение нефтеперерабатывающих заводов и трубопроводов может привести к дефициту источников энергии или катастрофе окружающей среды.

Комментарий специалиста

«Мы сильно зависим от Интернет. Любое злоумышленное вмешательство в эту среду может породить проблемы».

Карл Тайанен, председатель Центра сбора и анализа информации энергетики

№ 5. Отрасль: ФИНАНСЫ

Наихудший, но маловероятный сценарий

Сетевой червь может вывести из строя серверы и сети, используемые для осуществления разнообразных финансовых транзакций, что приведет к закрытию финансового рынка.

Более реалистичный сценарий

Кибератака, выводящая из строя компьютерные сети, в сочетании с физическим разрушением оборудования и линий связи может разрушить многие финансовые рынки и сделать их недоступными на значительно большой период.

Комментарий специалиста

«У нас все так взаимосвязано – платежные системы, клиринговые системы и прочие финансовые системы, что сбой в одной системе может оказать влияние на все остальные».

Сташ Джароки, председатель Финансовых служб ISAC

№ 6. Отрасль: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Наихудший, но маловероятный сценарий

Уязвимость в программном обеспечении может быть использована для получения доступа к критичным системам, которые могут использоваться для проведения атак на другие элементы информационной инфраструктуры или для создания широкомасштабных проблем со связью в Интернет.

Более реалистичный сценарий

Уязвимость в программном обеспечении может быть использована для получения доступа к критичным системам, которые могут использоваться для проведения атак на другие элементы информационной инфраструктуры.

Комментарий специалиста

«Сказать, что вы не видите возможности для осуществления разрушительной кибератаки, означало бы обманывать себя и не позволять нации обеспечить свою защиту».

Грег Эйкерс, президент IT-ISAC