Исследователи обнаружили уязвимость ЦОД к акустическим атакам.

Ученые из Университета Флориды и Университета электронных коммуникаций в Японии выявили потенциальную уязвимость подводных дата-центров перед звуковыми волнами, которые могут серьезно нарушить их работу.

Одним из заявленных преимуществ подводных дата-центров является использование окружающей водной среды для эффективного отвода тепла, что позволяет снизить эксплуатационные расходы на охлаждение серверов и прочего оборудования. Компания Microsoft экспериментировала с подводными дата-центрами в рамках своего проекта Natick , а компания Subsea Cloud предлагает коммерческий сервис. Китайский проект также находился в разработке по состоянию на конец прошлого года.

В недавно опубликованной статье на платформе arXiv исследователи подробно описывают , как звук на резонансной частоте жёстких дисков (HDD), установленных в погружных корпусах, может привести к снижению пропускной способности систем хранения RAID и даже к сбою приложений.

Такие акустические удары можно наносить на расстоянии до 6 метров от ЦОД. Ученые смоделировали ситуации с воздействием на системы только с HDD, а также на гибридные платформы с SSD и HDD. Они обнаружили, что звук правильной резонансной частоты вызывает вибрации в головках чтения-записи и дисках из-за распространения вибрации, пропорциональной акустическому давлению, что снижает их производительность.

Используя сервер Supermicro в конфигурации RAID 5 с HDD Seagate Exos 7E2 и SSD Intel D3-S4510, исследователи проводили испытания в металлических контейнерах в лаборатории и в открытых водоемах. Звук генерировался подводным динамиком. При воздействии на диски на разных частотах, включая 2, 3,7, 5,1–5,3 и 8,9 кГц, пропускная способность RAID-массива падала, причем в диапазоне 5,1–5,3 кГц наблюдалось «постоянное ухудшение пропускной способности». Уже через 2,4 минуты такого воздействия происходило значительное увеличение времени отклика баз данных на 92,7%, а некоторые жесткие диски выходили из строя.

Для проведения таких атак можно использовать специально оборудованные модули, соединенные с лодками или даже подводными аппаратами. Кроме того, подводные центры данных могут столкнуться с непреднамеренными помехами, например, от мощных гидроакустических сигналов подводных лодок.

Чтобы минимизировать риски от подобных угроз, исследователи рассмотрели несколько методов защиты. Один из предложенных методов — использование звукопоглощающих материалов для уменьшения вибрации, но это привело к повышению температуры работы серверов. Кроме того, оказалось, что атакующий может нейтрализовать этот метод, усиливая громкость звука.

Более эффективный способ защиты, предложенный в исследовании, включает использование модели машинного обучения для определения множественных снижений производительности на небольшом объеме данных. Это позволяет анализировать пропускную способность дисковых кластеров, расположенных близко друг к другу внутри подводного модуля.

После обнаружения проблем система управления ресурсами центра данных может применять методы репликации данных и корректирующего кодирования, чтобы перенаправить операции ввода-вывода на узлы, не затронутые акустическим воздействием, тем самым обеспечивая бесперебойную работу системы.