CLOUDFLARE®

Поиск путей решения проблем, связанных с цифровизацией индустрии здравоохранения

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

Содержание

Вступительная часть

Большинство задач, стоящих сегодня перед индустрией здравоохранения, связаны с возможностями обеспечения безопасности и ускорения работы онлайн-платформ здравоохранения, а также защиты персональных данных пациентов. Появление новых технологий, с одной стороны, повышает эффективность работы медицинских организаций, но с другой стороны, чревато возникновением новых факторов риска для безопасности.

Изменились также и ожидания потребителей. Пациенты предполагают, что смогут иметь виртуальный доступ к информации, смогут электронным способом записываться к врачам и получать консультации специалистов. Тем не менее, не все медицинские организации технологически готовы к таким переменам.

В период пандемии COVID-19 виртуальный доступ к медицинским услугам из роскоши превратился в насущную необходимость. Многие люди оказались заперты в своих домах, в очном формате услуги оказывались лишь в экстренных случаях. Результат: безопасность данных, эффективная и бесперебойная работа сети стали как никогда важны в здравоохранении.

Установленные на законодательном уровне требования к обеспечению конфиденциальности и защиты информации также влияют на то, как медицинским организациям приходится организовывать свою работу. В частности, в ЕС организации, оказывающие населению медицинские услуги, должны выполнять достаточно строгие требования к обеспечению конфиденциальности и защиты данных. Генеральным регламентом ЕС о защите персональных данных установлены минимальные требования к сбору и обработке личных данных - с наложением значительных штрафов в случае их невыполнения - параллельно Директивой по безопасности сетей и информационных систем установлены минимальные требования к информационной безопасности сети. Цена утечки данных пациентов довольно высока, причем на кону не только немалые финансовые затраты на восстановление данных и работоспособности системы, оплату штрафов, не следует забывать и о репутации организации, которая может быть безнадежно испорчена подобным инцидентом.

В этих условиях, в этом новом мире цифровых технологий, какой подход стоит взять на вооружение медицинским организациям для защиты своей информационной инфраструктуры?

В данной информационной брошюре будут раскрыты следующие темы:

- Текущие тренды в секторе здравоохранения и новые проблемы, вытекающие из них
- Требования, устанавливаемые законодательством в области обеспечения защиты и конфиденциальности данных
- Пути решения вышеуказанных проблем с соблюдением законодательных требований

Будущее здравоохранения - за цифровыми технологиями

Медицинские организации все больше используют для своей деятельности Интернет-технологии, которые применяются в разных формах. К числу текущих трендов цифровизации здравоохранения относятся электронные сервисы, возможность удаленной работы и защита удаленного доступа. Рассмотрим некоторые проблемы в области обеспечения безопасности данных и организации эффективной работы системы, связанные с этими трендами:

Дополнение и расширение сегмента электронных сервисов

В отчете консалтингового бюро McKinsey переход на виртуальный формат назван «следующей ступенью» развития современного здравоохранения.[1] Разумеется, есть такие услуги, которые могут быть оказаны только на личном приеме врачом, например, хирургическое вмешательство и осмотр пациента, в то же время есть много таких услуг, которые вполне успешно могут быть переведены в электронный формат. Эксперты McKinsey разделяют виртуально оказываемые медицинские услуги на три категории:

- Телемедицина: Сюда входит проведение в режиме реального времени видео-конференций «врач-пациент», видео-конференций с участием нескольких медицинских специалистов, а также обмен информацией по электронной почте и через файлообменники (вне формата реального времени).
- Цифровая терапия: Контроль возникновения побочных эффектов приема лечебных препаратов и использование программного обеспечения для консультации и снятия симптомов при ряде состояний.
- Навигация: Возможность безопасного доступа пациента к информации о своем здоровье, а также пакет онлайн-инструментов для поиска необходимых медицинских услуг и записи в соответствующие организации для получения этих услуг.

Подобные сервисы позволяют медицинским организациям экономить затраты и повышают комфорт пациентов при получении услуг этих организаций. В то же время, подобные электронные сервисы накладывают серьезные требования для медицинской организации в плане обеспечения необходимой технической и технологической базы для их оказания. Локальные, расположенные в самой организации дата-центры могут не справляться, когда речь заходит о расширении базы пациентов или переходе на удаленный режим работы сотрудников. Устаревшей IT-инфраструктуре может не хватить ресурсов для поддержки эффективного функционирования электронных сервисов.

Разразившийся на планете кризис в сфере здравоохранения, вызванный пандемией COVID-19, выявил необходимость расширения ассортимента электронных сервисов и усовершенствования IT-инфраструктуры. Оказавшись запертыми в своих домах, люди стали более зависимы от Интернета, ставшего основным инструментом получения необходимых им услуг. С декабря 2019 по апрель 2020 года потребление Интернет-трафика в развитых странах выросло на 40-50%, что связано со вспышкой COVID-19 в этот период.[2]

По мере того, как все большее количество людей перешли на Интернет в качестве источника получения самых базовых услуг, возросла и потенциальная угроза распределенных атак «denial-of-service» (отказ в обслуживании, они же DDoS-атаки), киберпреступность получила карт-бланш. DDoS-атаки являются одним из самых распространенных видов кибератак, в рамках такой атаки взломщики провоцируют перегруз приложения или сети колоссальным объемом трафика. В период печально известного локдауна в марте 2020 года, сеть захлестнула череда крупномасштабных (более 300 Гб/с) DDoS-атак.[3] В июне 2020 года компания Cloudflare автоматически нейтрализовала наиболее массивную DDoS-атаку, пик развертывания которой был зафиксирован на уровне 754 млн. пакетов данных в секунду.[4]

Заключение: Использующие онлайн формат оказания услуг медицинские организации должны быть готовы не только работать с соблюдением всех законодательных требований, но и быть технически готовыми к возросшему объему вредоносного трафика в рамках кибер-атак взломщиков. И чем в большей степени здравоохранение переходит на электронный формат оказания услуг, тем более очевидным это становится.

Рост популярности удаленной работы

Практика социального дистанцирования в период пандемии COVID-19 вынудила многие медицинские организации экстренно внедрить часть сотрудников, работающих удаленно. Хотя большинство врачей и медсестер могут работать только в очном формате, административный персонал, IT-специалисты и специалисты по ведению пациентов зачастую могут выполнять свои должностные обязанности удаленно. Кроме того, многие профильные врачи-специалисты в период эпидемии оказывали услуги удаленно - консультируя пациентов по телефону или через видео-конференции.[5]

Многие медицинские организации оказались не готовы к такому экстренному переходу на удаленный режим работы. Наиболее распространенной проблемой является обеспечение безопасного и гибкого доступа к внутренним приложениям. Сотрудники, работающие удаленно, зачастую вынуждены использовать для доступа к внутренним ресурсам организации свои личные мобильные устройства, не обеспеченные какой-либо защитой,[6] да и сами медицинские организации могут не иметь обеспеченных криптографической защитой каналов удаленного соединения (например, VPN-сетей), которые были бы установлены и настроены заранее, до кризиса COVID-19.[7]

Несмотря на все возникающие сложности, переход на удаленный режим работы - это состоявшаяся реальность, а не временная мера: многочисленные исследования показали, что политика «работай из дома» позволяет повысить КПД сотрудников.[8]

Обеспечение удаленного доступа

Большинство медицинских организаций по-прежнему работают на базе собственной локальной IT-инфраструктуры, что служит серьезным препятствием для работы, когда сотруднику нужен доступ к внутренним приложениям из дома. Располагающие такой локальной инфраструктурой медицинские организации могут применить следующие подходы к решению проблемы доступа при удаленной работе:

Организация удаленного доступа к рабочему компьютеру: Удаленный доступ к рабочему компьютеру подразумевает возможность удаленного подключения к основному рабочему ПК с отдельного устройства. Пользователи этой функции могут спокойно заходить в свой компьютер, открывать и редактировать файлы и использовать приложения, как если бы они действительно сидели за своим рабочим компьютером. Для реализации данной функции на устройствах сотрудников, пользующихся удаленным доступом, может потребоваться установка специальных программ-клиентов. Параллельно может встать вопрос об изменениях настроек корпоративных межсетевых экранов для контроля прохождения трафика между основным компьютером пользователя и подключенными извне устройствами.

Перенос в облачную среду: Новая технология Software-as-a-Service (SaaS) позволяет сотруднику получить доступ к функционалу приложений через облако и ресурсы Интернет. Перенос важнейших баз данных и приложений в облачную среду упрощает внедрение самой концепции «удаленной работы». Масштабирование базирующихся в облаке ресурсов также существенно упрощается. Однако, «переезд» в облако часто отнимает много времени и ресурсов. На сегодняшний день многие организации практикуют «гибридный» тип систем, в которых часть процессов перенесена в облако, а часть протекает в локальной сети. Соответственно, организация удаленного доступа в обеих направлениях - и в облаке, и в локальной сети - сопряжена с определенными трудностями.

Защита данных при удаленном доступе

Перед медицинскими организациями стоит задача - обеспечить сотрудникам, работающим удаленно, защищенный канал доступа к ресурсам, необходимым им для работы. Крайне важно, чтобы сотрудник мог работать с данными, не подвергая эти данные или системы, в которых они содержатся, риску кибератак.

В традиционно используемых предприятиями локальных системах за безопасности сети отвечает собственная команда IT-специалистов, которая следит за всеми подключаемыми извне устройствами. Помимо службы безопасности информационных систем в организациях обычно имеется служба физической безопасности, которая отвечает за контроль доступа сотрудников в помещение организации, и которая контролирует доступ к объектам внутренней инфраструктуры.

В случае сотрудников, работающих удаленно, такая структура не работает. Применение ресурсов в виде сотрудников, работающих удаленно, влечет за собой ряд угроз безопасности, в т.ч:

- **собственные устройства сотрудников могут быть не обеспечены необходимой защитой, что делает их уязвимыми перед кибератакой.** Периферийные устройства сети, подключаемые к ней извне, в частности, персональные устройства сотрудников, могут подвергнуться атаке, и им с легкостью может быть причинен ущерб, что позволит взломщикам похитить данные и использовать их для развертывания других видов атак на организацию.
- **Доступ к данным осуществляется на основе идентификации личности сотрудника.** Взломщики знают способы деперсонификации данных даже добросовестных пользователей, для этого существует масса способов, в том числе захват аккаунтов.
- **Каналами прохождения данных могут быть незащищенные сети.** При использовании Интернет-каналов существует риск того, что взломщики перехватят персональные данные в процессе передачи, когда они проходят через различные сетевые каналы соединения.

Организация безопасного доступа к ресурсам для сотрудников, работающих удаленно, обеспечит соблюдение нормативно-правовых требований в области защиты данных

Во многих регионах мира, в том числе там, где применяется Генеральный регламент ЕС о защите персональных данных, действуют законы, обязывающие медицинские организации принимать разумные и достаточные меры по защите персональных данных пациентов, которые они собирают и хранят у себя. Как правило, на персональные данные о здоровье индивида распространяются еще более жесткие требования по обеспечению их безопасности. Неприменение или некорректное применение мер безопасности может навлечь на организацию проблемы в виде специальных расследований и крупных штрафов.

Вообще, обеспечение безопасности персональных и медицинских данных - достаточно сложная задача для любой организации, а переход на удаленную работу еще больше усложняет ее.

По этой причине для сотрудников, работающих удаленно, крайне важно внедрить и использовать эффективные и надежные механизмы контроля доступа. Только уполномоченные и имеющие специальное разрешение лица должны иметь доступ к медицинским и персональным данным.

Помимо разработки дополнительных требований в рамках политики контроля доступа медицинские организации должны принять дополнительные меры по обеспечению безопасности и защите персональных данных своих пациентов.

- Защита данных в процессе передачи и в процессе хранения: При прохождении через сеть, в том силе по каналам Интернет-соединения, данные должны быть зашифрованы и защищены протоколом HTTPS, VPN-сетью или любым другим методом. Все сотрудники, хранящие данные на своих персональных устройствах, должны зашифровать свой жесткий диск.
- Защита периферийных устройств сотрудников: Установка антивирусного ПО - минимальное требование к защите используемых сотрудниками личных устройств.
  При работе удаленных сотрудников с сетью Интернет весьма полезны шлюзы информационной безопасности, которые защищают соединение.
- Защита от захвата персональных аккаунтов сотрудников: По возможности организации должны внедрять механизмы двухфакторной аутентификации для каждого приложения, официально используемого в сети организации. Именно двухфакторная аутентификация делает крайне сложным для взломщика получение доступа к персональному аккаунту сотрудника.

Почему медицинские организации стремятся шагать в ногу с последними достижениями в области цифровых технологий

Проблемы организационного характера

Когда заходит речь о защите данных и повышении качества обслуживания пациентов, медицинские организации часто сталкиваются с проблемой ограниченности бюджета и человеческих ресурсов. В ходе одного исследования выяснилось, что в большинстве больниц только 5% бюджета выделяется на решение проблем информационной безопасности. [9]

Нехватка ресурсов стала фактором, ограничивающим возможности создания и реализации единых стандартов информационной безопасности в рамках медицинских организаций. В результате, данные организации зачастую более уязвимы перед лицом киберугрозы. В 2019 году Управлением Комиссара по информации был озвучен доклад, согласно которому большинство инцидентов с утечкой данных было зафиксировано именно в секторе здравоохранения.[10] Более, чем в 60% случаев утечка данных была вызвана не кибератаками извне, а банальным человеческим фактором. Этот доклад соответствует выводам, сделанным экспертами компании Verizon в их собственном отчете по итогам расследований случаев утечки данных в 2019 году (Data Breach Investigations Report), согласно которому 59% случаев утечки данных произошли по вине самих сотрудников, а не в следствие кибератак.[11]

Дефицит знаний и поддержки на институциональном уровне является основной проблемой для медицинских организаций. Конечно, инициируемые извне кибератаки также являются угрозой, но при этом многие медицинские организации не располагают необходимой инфраструктурой для предотвращения и отражения таких атак.

Проблемы технического характера

Большинство медицинских организаций используют традиционную локально настроенную инфраструктуру сети. Такую инфраструктуру трудно масштабировать, а ее ресурсов может не хватать для организации работы электронных сервисов, нужных пациентам. При этом, полный отказ от этой инфраструктуры - тоже не выход для большинства медицинских организаций, что связано с недостаточным финансированием, невозможностью временно отключать ненужные сервисы для ввода в строй новых, а также с отсутствием поддержки на институциональном уровне.

Такая устаревшая инфраструктура оставляет медицинские организации безоружными в ситуациях, когда нужно справиться со скачками трафика и сложными видами кибератак. В условиях кризиса, вызванного пандемией COVID-19, произошел резкий скачок пользовательского трафика в связи с переходом огромного количества людей на электронные сервисы, и этот поток трафика буквально захлестнул оказавшиеся неготовыми к этому организации.

DDoS-атаки также могут вывести из строя всю инфраструктуру медицинской организации. Количество DDoS-атак в секторе здравоохранения возросло в период с 2017 до 2018 года, утроилось количество атак DDoS-атак, мишенью которых стали электронные сервисы SaaS и сторонние дата-центры.[12]

Проблемы и вызовы цифровой трансформации

Необходимость наличия устойчивого подключения к сети становится все более насущной проблемой в секторе здравоохранения на фоне растущего количества устройств Интернета Вещей, специализированных мобильных приложений и распространения облачных технологий. Задействование открытых Интернет-каналов создает угрозу для данных в секторе здравоохранения, делая их уязвимыми для взломщиков.

Кроме того, во всех отраслях наблюдается увеличение количества сотрудников, которые используют для работы личные мобильные устройства. По данным одного исследования, 86% сотрудников приносят на работу собственные устройства, и почти все эти сотрудники используют свои устройства для доступа к корпоративным аккаунтам электронной почты или другим внутренним приложениям.[13] Когда к защищенной внутренней сети подключается не обеспеченные защитой устройства, сеть тут же становится незащищенной или ее защита эквивалентна защите самого уязвимого из этих подключенных устройств. Таким образом, подключение к корпоративной информационной сети незащищенных персональных устройств делает эту сеть уязвимой для кибератак.

Проблемы, связанные с нормативно-правовым регулированием

Генеральный регламент ЕС по защите персональных данных в сфере здравоохранения

Данный Регламент вступил в силу 25 мая 2018 года,[14]в нем установлены требования к сбору, обработке и хранению персональных данных любого гражданина ЕС.

Одним из важных аспектов применения данного Регламента является то, что перечисленные в нем требования к организациям распространяются только на персональные данных граждан ЕС, независимо от того, где находится сама организация, а также где были собраны, обработаны или где хранятся эти персональные данные. Таким образом, любая медицинская организация, оказывающая услуги гражданам ЕС, независимо от своего местоположения и региона деятельности, должна соблюдать требования данного регламента.

Кроме того, данный Регламент расширяет само понятие персональных данных. В отдельные категории вынесены генетические данные, биометрические данные для уникальной идентификации физических лиц, а также данные касательно состояния здоровья - все эти данные определяются как специальные категории. На такие специальные категории данных распространяются дополнительные требования по обеспечению безопасности, согласно Регламенту. Помимо этого, согласно Регламенту, обработка всех персональных данных, особенно специальных категорий персональных данных, должна производиться с учетом требований обеспечения надлежащего уровня их безопасности. В результате медицинские организации будут вынуждены сначала принять необходимые меры и внедрить механизмы безопасности и технологии, пригодные для работы с такими категориями данных, а также реализовать их в своей политике защиты конфиденциальности информации.

Здравоохранение и Директива о безопасности сетей и информационных систем

В июле 2016 года Европейским Парламентом была утверждена Директива о безопасности сетей и информационных систем (Директива NIS), с этого момента все государства-члены ЕС должны интегрировать данную Директиву в свое национальное законодательство.[15]

В рамках Директивы предъявляются более жесткие нормативно-правовые требования к кибербезопасности для организаций, предоставляющих жизненно-важные и цифровые услуги. Поскольку некоторые медицинские организации были признаны поставщиками жизненно важных услуг, данные организации, в первую очередь, должны соблюдать все требования Директивы.

Такие организации-поставщики жизненно важных услуг обязаны внедрить у себя системы управления рисками. При наступлении инцидента, связанного с утечкой данных, они должны незамедлительно уведомлять об этом соответствующие надзорные органы в своей стране.

Что это означает для индустрии здравоохранения? Медицинские организации должны:

- **Обеспечивать защиту вверенных им данных.** Внедрять и применять технологии и процессы для обеспечения защиты данных и предотвращения их утечек.
- **Внедрять механизмы контроля доступа.** Многие инциденты, связанные с утечкой данных, произошли по вине собственных сотрудников, которые имели слишком обширный доступ к данным, а вовсе не потому, что некие неизвестные взломщики смогли прорваться сквозь все рубежи защиты.
- **Вы должны четко знать, к кому обратиться в случае наступления инцидента.** В каждой стране-участнице ЕС существует своя группа реагирования на инциденты в сфере информационной безопасности (CSIRT) или схожий по функциям орган. Медицинские организации должны быть готовы незамедлительно сообщить соответствующим инстанциям о произошедших инцидентах.

Разработки для решения актуальных проблем здравоохранения

Виртуальные медицинские сервисы - новая реальность нашего времени

Поскольку услуги здравоохранения относятся к категории жизненно важных, защита данных, которые циркулируют в организациях, оказывающих эти услуги, должна стать вопросом первостепенной важности. Электронные сервисы, с одной стороны, должны быть доступными, с другой стороны, безопасными. Это требует вложений в создание надежной цифровой инфраструктуры и защиты этой инфраструктуры от атак.

McKinsey рассматривает вопрос о том, какие меры по защите данных должны принять медицинские организации в свете изменений, произошедших в период кризиса COVID-19: «Проанализируйте свои виртуальные приложения, взаимодействие систем работы с пациентами (например, электронная медицинская карта, цикл учета доходов, цифровой ресепшн) и вспомогательную инфраструктуру. Определите подход, которым будете руководствоваться при переходе от экстренно организованных на период кризиса COVID-19 решений к формированию устойчивых, надежных и безопасных платформ для работы электронных медицинских сервисов».

Поскольку многие медицинские организации не располагают цифровой инфраструктурой, необходимой для организации работы электронных сервисов, им могут помочь в этом вопросе решения, предлагаемые сторонними организациями. В частности, применение сетей доставки контента (CDN) может улучшить производительность Интернет-каналов, повысить надежность и защитить от DDoS-атак на электронные сервисы. Сети доставки контента CDN могут интегрироваться с дополнительными сервисами безопасности для защиты персональных данных пациентов и поддержания надежного функционирования систем.

Обеспечение технической поддержки и защиты данных для сотрудников, работающих удаленно

Облачные решения для удаленной работы

Раньше для обеспечения безопасности, надежности и эффективности функционирования локальной IT-инфраструктуры предприятия применялись полностью аппаратные решения. При этом сотрудникам, работающим удаленно необходимы более гибкие решения, основанные на применении облачных технологий.

Например, локальный межсетевой экран может защитить внутренние сети и дата-центры от кибератак. Но этот же межсетевой экран окажется неэффективным при защите веб-каналов, приложений в концепции SaaS или данных в этих приложениях, на участке между периферийными устройствами пользователей и внутренними корпоративными серверами. Для этих случаев наиболее эффективным решением будет межсетевой экран для веб-приложений, шлюз информационной безопасности и криптозащита в рамках протокола HTTPS.

Для защиты персональных данных и устройств сотрудников, работающих удаленно, медицинским организациям следует остановить свой выбор на разработчиках, чья продукция поддерживает разные типы IT-инфраструктуры, в том числе, локальную, облачную и гибридную.

Продукты безопасности для сотрудников, работающих удаленно

Существует целый ряд инструментов для управления идентификацией и доступом (identity and access management (IAM), которые помогают снизить риски и обеспечить безопасность устройств сотрудников, работающих удаленно, а также защитить конфиденциальные данные.

Шлюз информационной безопасности: Шлюзы информационной безопасности «вбиты» на участке между внутренними пользователями сети и незащищенными сетями Интернета. Они позволяют фильтровать подозрительный контент, поступающий в объеме веб-трафика, для нейтрализации киберугроз и предотвращения утечки данных. С их помощью также можно блокировать пользователей, чье поведение вызывает подозрения или неавторизованно.

В шлюзах информационной безопасности применяется механизм DNS-фильтрации или URL-фильтрации для блокировки вредоносных веб-сайтов, антивирусы для предотвращения компрометации периферийных устройств, системы предотвращения утечек данных (DLP), не позволяющие выводить данные за границы безопасного периметра, а также другие формы нейтрализации киберугроз. Например, некоторые виды шлюзов информационной безопасности способны вычленять в составе исходящего трафика конфиденциальные данные - при попытках вывода этого трафика из периметра безопасности - таким образом, предотвращается утечка данных.

Контроль доступа: Инструменты контроля доступа помогают предотвращать утечки персональных данных пациентов путем отслеживания и управления доступом внутренних пользователей к системам и данным. Внедрение таких инструментов позволяет разумно ограничивать доступ врачей, медсестер, администраторов и прочих сотрудников к внутренним системам, предоставляя его только в рамках их полномочий и предотвращая несанкционированный доступ к этим системам.

Система контроля доступа с единой аутентификацией (SSO): Сотрудники, работающие удаленно, часто предпочитают пользоваться приложениями в концепции SaaS, вместо тех, что установлены локально на их собственных устройствах, доступ к приложениям в концепции SaaS они получают через обычный браузер. При этом необходимость осуществления отдельной процедуры входа для каждого из этих приложений приводит к тому, что пользователи начинают придумывать самые простые пароли, не обеспечивающие защиты, эта схема осуществления доступа также с трудом контролируется со стороны IT-специалистов организации. SSO позволяет пользователю авторизоваться только один раз для входа и доступа ко всем приложениям в концепции SaaS.

Механизмы мультифакторной аутентификации (MFA): Для сотрудников, работающих удаленно, необходимы надежные механизмы аутентификации, поскольку физически проверить личность пользователя, что легко достижимо при его личном присутствии в офисе, клинике или больнице, не представляется возможным. Разгадать можно даже самые надежные пароли, однако механизм мультифакторной аутентификации позволяет минимизировать риск компрометации аккаунта даже в случае, если взломщик завладеет паролем. Применение дополнительных средств аутентификации, помимо пароля, ставит перед взломщиком непростую задачу - чтобы завладеть аккаунтом придется изобрести способ обхода этого дополнительного барьера аутентификации.

Cloudflare для здравоохранения

Защитите приложения и сети от вредоносных атак

По мере роста цифровизации и зависимости от Интернет-технологий в индустрии здравоохранения, атаки на приложения и сети становятся обычным делом. Разработанные компанией Cloudflare решения в области безопасности обеспечивают комплексную защиту как для персональных данных пациентов, так и для приложений, с которыми они работают. Продукты компании Cloudflare помогают медицинским организациям защитить свои веб-приложения и локальные сети от DDoS-атак, вредоносных ботов и прочих критических уязвимостей.

Организация оперативных и надежных в функционировании электронных сервисов (цифровое присутствие)

От анализа медицинских карт до проведения видео-конференций со специалистами - пациенты ожидают бесперебойного качества обслуживания. Разрабатываемые компанией Cloudflare продукты помогают повысить надежность и эффективность функционирования сети, они служат для обработки запросов, кеширования статического контента и «умной» маршрутизации трафика по периферии сети, ускоряют работу электронных сервисов и делают их функционирование бесперебойным.

Продукты Cloudflare обеспечивают высокую удовлетворенность пользователей при работе с сетью за счет быстрой и эффективной маршрутизации трафика - качество работы сети всегда отличное, независимо от типа пользовательского устройства, его местоположения и скорости Интернета. С продуктами Cloudflare ваши веб-приложения всегда остаются онлайн и эффективно работают даже в период пиков трафика или в случае DDoS-атак.

Отдел регионального обслуживания Cloudflare Regional Services позволяет клиентам контролировать обслуживание своего трафика, выбрав ближайший офис из списка доступных более, чем в 200 городах и 100 странах мира.

Защита внутренних информационных ресурсов в виде устройств, сетей и приложений

По мере распространения электронных сервисов в сегменте здравоохранения, а также на фоне глобального перехода к формату удаленной работы, национальные границы в отрасли здравоохранения постепенно стираются. Это означает наличие доступа к ценным конфиденциальным данным из любой точки. Продукт Cloudflare for Teams обеспечивает защиту устройств, сетей и внутренних приложений в режиме «единого окна». Он позволяет IT-специалистам обеспечить безопасный доступ к внутренним приложениям без применения VPN, а также предотвратить утечку информации до того момента, как ее масштабы потребуют вмешательства на уровне политики безопасности всей сети.

Заключение

Для повышения качества обслуживания пациентов медицинские организации все шире применяют в работе электронные сервисы, их популярность постоянно растет. При этом речь идет не только о хранении и обмене данными электронных медкарт, но и об оказании ряда медицинских услуг в формате онлайн. Такой технологический скачок неизбежно поднимает вопрос о защите данных и эффективности работы Интернет-каналов.

В ЕС для медицинских организаций крайне важно обеспечить готовность обслуживать пациентов по всей территории Евросоюза, в разных странах, без учета национальных границ. Медицинские организации должны знать о действующих в регионе присутствия законодательных требованиях в области защиты данных, и соблюдать их. Они должны быть готовы помимо организации качественных и бесперебойно функционирующих сервисов обеспечить безопасность вверенных им персональных данных пациентов.

Продукты компании Cloudflare дают возможность медицинским организациям на территории ЕС обеспечить качественное, безопасное и бесперебойное обслуживание пациентов, а также эффективно организовать работу сотрудников и поставщиков.

Чтобы начать сотрудничать с компанией Cloudflare, вы можете отправить заявку по электронной почте: enterprise@cloudflare.com

Примечания

1. Дженнифер Фоукс и со-авторы «Виртуальные медицинские услуги: Взгляд на следующий уровень оказания услуг здравоохранения.» McKinsey & Company, 11 июня 2020 года, https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/virtual-health-a-look-at-the-next-frontier-of-care-delivery#. Проверено 25 августа 2020 года

2. Джон Грэхэм-Камминг «Производительность работы сети в период чрезвычайной ситуации, вызванной пандемией COVID-19.» Cloudflare, 23 апреля 2020 года, https://blog.cloudflare.com/recent-trends-in-internet-traffic/. Проверено 25 августа 2020 года

3. Омер Йоачимик и Арун Сингх «Новые тенденции развертывания DDoS-атак сетевого уровня в 1-ом квартале 2020 года.» Cloudflare, 15 мая 2020 года, https://blog.cloudflare.com/network-layer-ddos-attack-trends-for-q1-2020/. Проверено 25 августа 2020 года

4. Омер Йоачимик «Как автоматически нейтрализовать DDoS-атаку в объеме 754 миллиона пакетов данных в секунду». Cloudflare, 9 июля 2020 года, https://blog.cloudflare.com/mitigating-a-754-million-pps-ddos-attack-automatically/. Проверено 25 августа 2020 года

5. Кевин Шарнхорст «Кибербезопасность в сфере здравоохранения в свете изменений, вызванных пандемией COVID-19: Лучшие практические рекомендации для сотрудников, работающих удаленно». Health Catalyst, 25 марта 2020 года, https://www.healthcatalyst.com/insights/covid-19-healthcare-cybersecurity-remote-work-safety. Проверено 25 августа 2020 года

6. Кари Лидстоун «Топ 4 рекомендации для руководителей медицинских организаций по решению проблем, возникших в связи с переходом на удаленную работу». Med Tech Solutions, 22 апреля 2020 года, https://medtechsolutions.com/blog/top-4-tips-for-healthcare-it-managers-to-address-new-remote-worker-challenges/. Проверено 25 августа 2020 года

7. Майк Чэпл «5 способов защитить персональные устройства и данные для сотрудников в индустрии здравоохранения, работающих удаленно». HealthTech, 24 апреля 2020 года, https://healthtechmagazine.net/article/2020/04/5-ways-protect-devices-and-data-remote-healthcare-work. Проверено 25 августа 2020 года

8. Николас Блум и со-авторы «Насколько работа на дому оправдывает себя? Результаты китайского эксперимента». Oxford Academic, Ежеквартальный экономический вестник, том 130, № 1, февраль 2015 года, 20 ноября 2014 года, https://academic.oup.com/qje/article-abstract/130/1/165/2337855. Проверено 25 августа 2020 года

9. Макензи Гэррити «5% IT-бюджета стационаров идет на нужды кибербезопасности, при этом 82% стационаров сообщают об утечках персональных данных». Becker's Hospital Review, Becker's Health IT, 12 марта 2019 года, https://www.beckershospitalreview.com/cybersecurity/5-of-hospital-it-budgets-go-to-cybersecurity-despite-82-of-hospitals-reporting-breaches.html. Проверено 25 августа 2020 года

10. Тэмми Лавл «По данным статистики, именно в секторе здравоохранения наблюдается наибольшее количество инцидентов, связанных с утечкой персональных данных». Healthcare IT News, 28 августа 2019 года, https://www.healthcareitnews.com/news/europe/statistics-reveal-healthcare-sector-most-affected-personal-data-breaches. Проверено 25 августа 2020 года

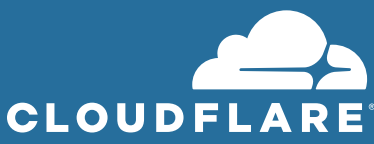
11. «Отчет по результатам расследований инцидентов с утечкой данных в 2019 году: Краткий обзор». Verizon, https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf. Проверено 25 августа 2020 года

12. Фред Донован «Количество DDoS-атак в секторе здравоохранения вышло на рекордную отметку в 2018 году». HIT Infrastructure, 21 марта 2019 года, https://hitinfrastructure.com/news/healthcare-ddos-attacks-on-organizations-edged-up-in-2018. Проверено 25 августа 2020 года

13. Элистер Джонсон «Популяризация концепции BYOD в бизнесе». ITSP Magazine, 1 ноября 2018 года, https://www.itspmagazine.com/from-the-newsroom/byod-for-business-is-on-the-rise. Проверено 25 августа 2020 года

14. «Документ 32016R0679.» EUR-Lex, https://eur-lex.europa.eu/eli/reg/2016/679/oj. Проверено 25 августа 2020 года

15. «Директива о безопасности сетей и информационных систем» (Директива NIS) European Commission, статья «Формируя цифровое будущее Европы»: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive. Проверено 25 августа 2020 года



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

РЕДАКЦИЯ: 15.09.2020