White Paper

Кибербезопасность в здравоохранении

Содержание

Введение

Несмотря на то, что организации повсеместно сталкиваются с киберугрозами, которые продолжают расти по сложности и объему, ни одна отрасль не является такой значимой мишенью и не подвергается таким атакам, как здравоохранение.

Помимо больниц, современная индустрия здравоохранения включает в себя производителей медицинского оборудования, производителей фармацевтических препаратов и биотехнологических организаций. Современная отрасль здравоохранения все больше зависит от цифровизации, и средства управления данными. Конфиденциальность остается главным приоритетом для руководителей высшего звена и их организаций в целом.

Данные, состоящие из информации о персонале и пациентах, технологические ноу-хау пользуются большим спросом у преступных группировок, государств и других субъектов. Независимо от покупателя информации, медицинские данные - это актив, для которого киберпреступники ищут различные способы монетизации.

Если вас все еще нужно убедить, подумайте о том, что в 4 квартале 2020 года число атак с использованием вредоносного ПО на медицинские учреждения выросло на 350% , в то время как 90% больниц и медицинских учреждений подверглись кибератакам по электронной почте в 2020 году.
Во время пандемии COVID-19 индустрия здравоохранения стала жертвой бесчисленных атак со стороны киберпреступников, наживающихся на хаосе.

Если отрасль здравоохранения хочет выжить в условиях неминуемых атак, она должна значительно усилить свою систему информационной безопасности.

В данном буклете рассматриваются вопросы, с которыми сталкиваются руководители высшего звена в секторе розничной торговли и электронной коммерции, предлагаются идеи и рекомендации по решению проблем.

В современном ландшафте кибербезопасности базовые методы предотвращения угроз информационной безопасности уже не работают. Не проходит и недели без очередного громкого взлома и его финансовых последствий, о которых сообщают СМИ. Но почему ритейлеры все еще подвергаются взломам, несмотря на объем инвестиций в продукты безопасности? Даже самые крупные розничные компании остаются уязвимыми, несмотря на наличие передовых решений SIEM и защиты конечных точек.

Мы рассмотрим вопрос почему розничные компании всех размеров должны предпринимать проактивные шаги для управления своими киберрисками.

Почему отрасль здравоохранения становится целью для атак?

Не секрет, что медицинские учреждения отстают в мерах безопасности по сравнению с банками и другими финансовыми организациями, которые, как правило, давно внедрили надежные процедуры кибербезопасности и технологии анализа угроз.

Это делает отрасль здравоохранения привлекательной целью для киберпреступников. Сложная структура управления в государственных учреждениях системы здравоохранения может привести к отсутствию определенных требований, недостаточной подготовке к кибератакам и трудностям в оценке устойчивости ИТ-активов. С другой стороны, организации, частные учреждения могут оставаться гибкими, адаптируемыми и лучше подготовленными к изменению или модернизации своих мер безопасности.

Однако частные медицинские организации, не имеющие государственной структуры, поддерживающей их, к лучшему или худшему, в большинстве своем просто не могут уделять приоритетное внимание инвестициям в кибербезопасность по сравнению со многими другими нюансами, которые возникают при поддержании частного предприятия. В результате многие частные медицинские учреждения оказываются совершенно неподготовленными к кибератакам

Для преступников, которые пытаются атаковать медицинские учреждения, достаточно нескольких недостатков в системе безопасности для того, чтобы скомпрометировать все ИТ-активы и системы.

Низкая осведомленность

Практики кибербезопасности, внедряемые организациями из сферы здравоохранения, часто воспринимаются как неудобства для перегруженных работой врачами и медсестрами, у которых нет времени на внедрение новых процедур безопасности в их и без того напряженную рабочую жизнь. Для того чтобы меры безопасности соблюдались, командам руководителей было бы разумно вписать новые меры безопасности в существующую практику, чтобы минимально нарушать работу или отвлекать медицинский персонал, однако зачастую это не так. В результате медицинские работники часто отдают предпочтение своим обязанностям перед надежной системой безопасности, оставляя дверь открытой для злоумышленников.

Нехватка кадров

Отрасль здравоохранения сталкивается с масштабной нехваткой киберспециалистов. В связи с бюджетными ограничениями большинство организаций отрасли здравоохранения не могут получить доступ к специалистам по кибербезопасности или обучить имеющийся персонал.

Бюджетные ограничения

Несмотря на громкие нарушения, которые привели к огромным финансовым потерям и поставили под угрозу жизни пациентов, очевидно, что безопасность все еще не является важным направлением для организаций отрасли здравоохранения. Организации здравоохранения, несомненно, будут оставаться восприимчивыми к вредоносным программам, DDoS, APT и другим угрозам.

Как киберпреступники зарабатывают на медицинских данных?

Данные компаний из отрасли здравоохранении сами по себе не более ценны, чем другие незаконно полученные данные. Отличительной чертой этих данных от других является их влияние на лечение пациентов (например, при невозможности воспользоваться информацией после атаки вируса-шифровальщика), а также срочность, с которой медицинские организации должны устранять любые нарушения в их ИТ-системах.

Очевидно, что такие данные очень востребованы киберпреступниками и другими субъектами угроз. Для защиты этих данных крайне важно, чтобы ИТ-специалисты начали понимать, что делает их данные ценным товаром и как киберпреступники будут использовать их для получения прибыли.

Персональные данные

По сравнению с данными, которые обычно похищают при нарушениях в финансовой отрасли, медицинские данные также содержат такие данные, как номер ОМС, номер паспорта и адрес электронной почты и пр. Эта информация представляет ценность для хакерских группировок, которые готовы хорошо заплатить злоумышленникам в обмен на ПД, чтобы затем использовать их в злонамеренных целях.

Интеллектуальная собственность

Интеллектуальная собственность (ИС) в сфере здравоохранения принимает форму патентов и товарных знаков, обычно относящихся к университетам или медицинским центрам, проводящим клинические испытания, фармацевтическим или биотехнологическим организациям, проводящим важнейшие исследования и разработки лекарств, или более мелким организациям, разрабатывающим новые устройства, процедуры или методики. ИС может быть украдена с целью выкупа или продана за конкурентам.

Репутационный ущерб

Интеллектуальная собственность (ИС) в сфере здравоохранения принимает форму патентов и товарных знаков, обычно относящихся к университетам или медицинским центрам, проводящим клинические испытания, фармацевтическим или биотехнологическим организациям, проводящим важнейшие исследования и разработки лекарств, или более мелким организациям, разрабатывающим новые устройства, процедуры или методики. В самом критическом случае ИС может равняться миллиардам долларов, вложенным в исследования и инвестиции, или быть крайне важной для будущего организации. ИС может быть украдена с целью выкупа или продана конкурентам.

Киберугрозы

В этом разделе мы постараемся осветить некоторые из современных киберугроз, нацеленных на сектор здравоохранения.

Вредоносное ПО

Вредоносное ПО - это общий термин для вредоносных программ (вирусы, черви, боты, руткиты, шпионские программы и программы-вымогатели) , устанавливаемых злоумышленниками, в результате того, что пользователи неосознанно устанавливают код или программу, которая дает злоумышленникам контроль над их системой. Чаще всего это происходит через приложения для обмена сообщениями или вложения электронной почты, которые устанавливают вредоносные программы, способные блокировать серверы, красть информацию или отменять исправления, оставляя системы уязвимыми для последующих угроз.

Одна из форм вредоносного ПО - программы-вымогатели, предназначенные для предоставления злоумышленникам полного контроля над системой пользователя или организации, который будет удерживаться до тех пор, пока жертвы не заплатят выкуп за разблокировки данных. Программы-вымогатели часто проникает в системы через успешные фишинговые атаки.

Согласно исследованиям, , трояны являются наиболее эффективными формами вредоносного ПО при атаках на системы здравоохранения (79%), за ними следуют программы-вымогатели (18%) и шпионские программы (3%).

Многие мобильные приложения, используемые в сфере здравоохранения пациентами и сотрудниками, уязвимы к подобным угрозам, несмотря на предполагаемые меры безопасности. Сегодня через мобильные приложения проходит больше медицинских данных, чем когда-либо, и этот показатель продолжает расти.

Рост числа подключаемых устройств в медицинских учреждениях усугубляет проблемы безопасности, “растягивая” меры безопасности среди внутренних, внешних и BYOD устройств и увеличивая возможности злоумышленников.

Фишинг

Фишинг остается основным вектором атак. Он широко распространен среди тех, кто атакует медицинские учреждения с целью успешной кражи персональных данных или открытия бэкдора для других угроз, таких как программы-вымогатели.

Злоумышленники под видом сотрудника или партнера организации обманывают получателей электронной почты, заставляя их отвечать на поддельные сообщения или предпринимать какие-либо действия. Пациенты также могут стать жертвами вредоносных фишинговых писем.

Киберпреступники используют пандемию Covid-19 для кражи информации через фишинговые письма, оформленные как письма от медицинских учреждений.

Согласно исследованиям, в этом году уже было создано более 86 000 доменов, связанных с коронавирусом, три процента из которых были признаны вредоносными, а пять процентов - подозрительными.

Уязвимости третьих сторон

Хотя компании должны вкладывать значительные средства в собственную инфраструктуру кибербезопасности, сторонние поставщики могут стать слабым звеном в системе обеспечения безопасности.

Взлом ИТ-инфраструктуры клиентов, подрядчиков и партнеров может позволить злоумышленникам проникнуть в сеть медицинских учреждений или получить данные принадлежащие организации.

Хактивизм

Как и все органы государственного сектора, больницы и аналогичные медицинские учреждения подвергаются риску стать мишенью для хактивистов, использующих кибератаки для протеста или продвижения определенной политической точки зрения.

Управление рисками кибербезопасности

Ни одна организация не может полностью защититься от всего спектр киберугроз. Данные, сети и приложения становятся мишенью для киберпрестуников. Поэтому нужно ставить следующим образом: “когда”, а не “если”.

Чтобы противостоять этим вызовам, медицинские организации должны создавать проактивные меры безопасности, которые помогут им быстро обнаруживать и реагировать на инциденты.

Взаимодействие на уровне руководства

Прежде всего, руководство компании должно быть полностью вовлечено в процесс кибербезопасности. Защита предприятия от постоянно меняющегося динамического ландшафта угроз больше не является прерогативой ИТ-директора, CISO или ИТ-команды. Кибербезопасность - это работа каждого, и руководство компании несет ответственность за создание и поощрение вовлечения к снижению киберрисков во всем бизнесе.

Необходимо убедиться, что сотрудники, прямо или косвенно вовлеченные в любые проекты, связанные с риском для бренда, включают оценку безопасности в каждое из действий, проектов и процессов.

В целом, очень важно создать сильную культуру кибербезопасности в организации. Она должна распространяться от руководящего состава вплоть до новых сотрудников, поощряя их к полному пониманию рисков, связанных с использованием определенных технологий.

Обучение

Помимо руковдства, организации должны обеспечить, чтобы все сотрудники имели базовое представление о киберрисках и понимали свою личную ответственность за защиту данных пациентов и организации. Для создания такой культуры безопасности медицинские работники всех уровней должны регулярно проходить обучение и тренинги по кибербезопасности. Такое обучение жизненно важно для предоставления сотрудникам инструментов, позволяющих выявлять и реагировать на сложные атаки. Этому может способствовать регулярное проведение тестов по кибербезопасности для выявления слабых мест и проведения специального обучения по ним.

Защита устройств

Поскольку медицинские работники все больше полагаются в своей работе на мобильные и IoT-устройства, а все больше пациентов взаимодействуют с медицинскими работниками через цифровые каналы, необходимость защиты этих устройств является одним из главных приоритетов для отрасли здравоохранения, так как расширение возможностей подключения означает увеличение возможностей для проникновения злоумышленников в организацию. О

Организациям будет полезно использовать строгую политику защиты устройств в рамках управления рисками, чтобы позволить медицинскому персоналу безопасно использовать имеющиеся у них девайсы. Это включает в себя аутентификацию пользователей, шифрованную связь, контроль доступа на основе ролей и виртуальные частные сети для предотвращения проникновения злоумышленников в сеть.

В дополнение к сетевым нарушениям, субъекты угроз также могут получить доступ к данным путем кражи физических устройств. Организации должны разработать стратегию для обеспечения безопасности медицинских данных, IP и ценных данных пациентов и персонала, доступных через подключенные устройства. Это означает строгие политики, предписывающие, чтобы любое устройство было надлежащим образом защищено и не покидало физический периметр.

Сотрудничество и обмен знаниями

Подчеркнем важность обмена оперативной информацией об угрозах в секторе здравоохранения. Руководители должны при любой возможности взаимодействовать со своими коллегами в отрасли здравоохранения, обмениваться знаниями, решениями и опытом, чтобы внедрять передовую практику кибербезопасности в отрасли и гарантировать, что то, что проникает в одну организацию, не будет допущено в другую.

Постоянный мониторинг и расследование угроз

Непрерывный мониторинг - это средство, с помощью которого внешние риски для организации оцениваются практически в режиме реального времени, что позволяет принимать решения благодаря актуальной информации.

Мониторинг в режиме реального времени также позволяет эффективно управлять угрозами, используя информацию из нескольких источников через динамический поток, что помогает снизить коэффициент ложных срабатываний. Кроме того, непрерывный мониторинг позволяет лицам, принимающим решения в области безопасности, более эффективно распределять ресурсы безопасности, действовать на опережение перед лицом будущих атак и улучшать периметр безопасности в масштабах всей организации.

План реагирования на инциденты

Поскольку кибератаки все больше воспринимаются как неизбежность, а угрозы для отрасли здравоохранения становятся все более серьезными, нет никаких оправданий тому, что у вас нет готового плана реагирования инциденты. Этот план действий в чрезвычайных обстоятельствах, в идеале подкрепленный автоматизированной аналитикой угроз, поможет значительно ограничить или полностью избежать последствий будущих атак, и медицинские учреждения не должны ждать, пока станет слишком поздно, чтобы разработать такой план.

Заключение

Чтобы противостоять растущему преступному интересу к этой отрасли, медицинские организации должны повысить уровень безопасности, внедряя культуру безопасности на всех уровнях и формируя понимание действующей защиты и ожидаемых последствий в случае ее несоблюдения. В этом документе описаны текущие угрозы, стоящие перед индустрией здравоохранения, и стоящие за ними субъекты угроз.

Чем мы можем Вам помочь?

ООО «НТЦ ЕВРААС», являясь многопрофильной коммерческой структурой, имеет все необходимые лицензии регуляторов рынка информационной безопасности, в том числе лицензии на осуществление работ с использованием сведений, составляющих государственную тайну.

Обладая фундаментальными знаниями и опытом в области защиты информации, эксперты НТЦ «ЕВРААС» предлагают новейшие комплексные разработки в сфере обеспечения безопасности компаний розничной торговли.

Мы проектируем системы под конкретные нужды и специфику организаций, тем самым гарантируя, что система информационной безопасности комплексно решает все задачи и обеспечивает надежную круглосуточную защиту ваших корпоративных ресурсов и данных.

Контакты:

г. Москва, ул. Автозаводская 13/1

8 (495) 748-09-44

evraas@evraas.ru