Кибер-пандемия

Компьютерные атаки в сфере здравоохранения

pandasecurity.com

panda

Кибер-пандемия

Нет другой отрасли, которую можно было бы рассматривать в качестве более благородной и беззаветной, нежели здравоохранение. Это настолько гуманитарная сфера, что даже в конфликтных ситуациях ее представители обязаны уважать и защищать Вас любым доступным способом. Сложно поверить, что кто-то хотел бы подорвать общественное значение здравоохранения, не говоря уже о том, что кто-то преднамеренно осуществляет кибер-атаки против медицинских организаций.

Деньги - то, что движет миром, но, к сожалению, для них неважна специфика отрасли. Деньги - это основная мотивация для большинства кибер-преступников, кто смог обнаружить в здравоохранении "кладезь" уязвимостей.

Здравоохранение сфокусировано на других жизненно важных вопросах, возможно по этой причине медицинские организации долгое время не обращали должного внимания на свою IT-безопасность. В итоге данная отрасль обеспечена высокотехнологичными решениями с недостаточным уровнем IT-безопасности, что крайне сильно нас тревожит.

Опасное окружение

Шифровальщики сегодня стали одной из самых распространенных угроз - вот еще один пример того, что деньги - это основной драйвер для кибер-преступников. Атака на тех, кто обладает ценной информацией, и кто готов заплатить выкуп, - все это сделало шифровальщики идеальным оружием.

Мы видели атаки против определенных отраслей. На самом деле, интерес хакеров к некоторым секторам экономики, например, финансы, вполне очевиден: опустошить банковские счета. Даже когда жертва - банк, цель все та же, что мы недавно наблюдали в случае с Центральным банком Бангладеш.

Другие отрасли не могут страдать от прямого воровства денег, но цель все также ясна. Как было показано в недавней белой книге “Хакеры отелей”, кибер-атаки на магазины, сервисные компании и отели позволили заразить их POS-терминалы, чтобы украсть деньги с банковских карт их клиентов.

Впрочем, в здравоохранении мотив не столь очевиден. Во многих странах пациентами не принято использовать банковские карты для оплаты медицинских услуг, потому как они оплачиваются страховыми компаниями. И все же больницы все чаще становятся жертвами кибер-атак.

Почему больницы стали целью кибер-преступников?

По данным Управления гражданских прав в США, **в течение 2015 года зафиксированы 253 дыры безопасности в секторе здравоохранения, в результате чего было украдено свыше 112 миллионов записей**. По данным IBM, этот сектор экономики в 2015 году чаще других отраслей подвергался кибер-атакам.

Здравоохранение - это сердце технологической революции. Отрасль переходит на хранение всей информации в электронном виде, что, несомненно, выгодно для пациентов и больниц.

Данная информация доступна в сети и она полезна в том случае, если у пациента меняется врач, который легко может ознакомиться с историей болезни. Такое удобство одновременно породило серьезную проблему безопасности для всей отрасли. Медицинская информация очень ценна и высокочувствительна, поэтому тот, кто контролирует ее, может серьезно разбогатеть.

В некоторых странах Вы можете продать эту украденную информацию, причем есть даже компании, которые заинтересованы в покупке таких данных (исследовательские центры и страховые компании). Тогда, конечно, есть "черный рынок", где медицинская информация может быть более ценной, чем данные банковской карты.

Медицинские документы содержат огромный объем персональной информации, которая может использоваться как "мастер-ключ" для будущих атак. Например, высокопоставленные лица, кто особенно осторожен в отношении своей конфиденциальности, и не разглашает личную информацию в Интернете, соцсетях и пр. Даже они не могут предотвратить хранение своих записей в файлах медицинских центров. Если эта конфиденциальная информация попадет в чужие руки, их личные данные перестанут быть тайной.

Другим примером может быть получение доступа к конфиденциальной информации в фармацевтических центрах, когда компании готовы платить большие деньги за возможность "увести" патент от конкурента. Или возможность получения личной информации, принадлежащей врачу, для незаконной выписки рецепта.

Истории болезней, результаты анализов, адреса почты, пароли, номера соцстраховок, конфиденциальная информация сотрудников, пациентов и компаний: все это очень ценная информация. Проблема в том, что **медицинские организации защищены устаревшими системами безопасности**.

История прибыльных атак

Красный Крест (США)

В 2006 году сотрудник Красного Креста в Сент-Луисе (США) украл идентификаторы и информацию о трех донорах крови. Последствия могли быть гораздо серьезней, т.к. этот сотрудник имел доступ к данным более чем 1 миллиона доноров.

Доступ к данным более 1 миллиона доноров

Temple Street Children's University Hospital (Ирландия)

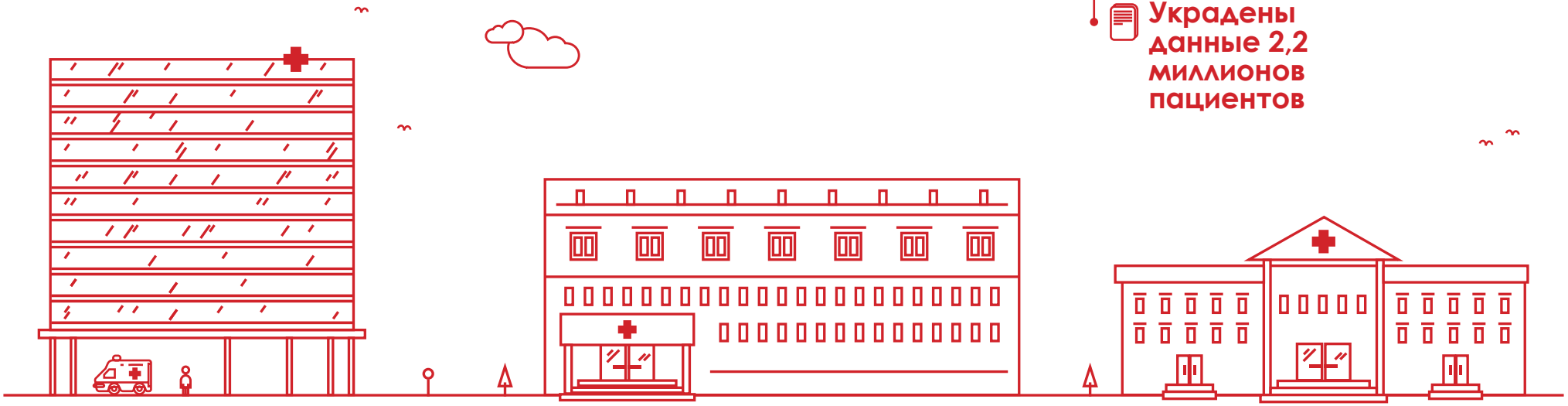
Спустя год в Ирландии из Temple Street Children's University Hospital было украдено два сервера, содержащие данные почти 1 миллиона пациентов, включая ФИО, дату рождения и причины пропуска занятий.

Украдены данные 1 миллиона пациентов

Госпитали и клиники Университета Юта (США)

В 2008 году госпитали и клиники Университета штата Юта (США) заявили о краже данных 2,2 миллионов пациентов. Данные хранились на пленочных носителях, которые были оставлены в машине одного из сотрудников внешней компании-подрядчика. В этом случае сотрудник не выполнил установленные процедуры для транспортировки информации, а потому была украдена персональная информация свыше 2 миллионов людей.

Украдены данные 2,2 миллионов пациентов



До сих пор мы обсуждали только конкретные, не массовые атаки. Однако с годами серьезно ситуация меняется. **По данным исследования, опубликованного Ponemon Institute, за последние 5 лет число атак в здравоохранении увеличилось на 125%. Кибер-атаки стали основной причиной потери информации.**

Это вызывает беспокойство, особенно если учесть, что 91% организаций, рассмотренных в этом исследовании, хотя бы раз за последние 2 года были атакованы, что привело к потере данных. 40% признались, что за этот период столкнулись с пяти и более случаями потери данных.

Страховая компания Anthem (США)

Одна из самых серьезных атак в этом секторе случилась в феврале 2015 года. Вторая крупнейшая страховая компания в США, Anthem, пострадала от атаки, приведшей к краже 80 миллионов записей о пациентах, в которых содержались критически важные данные (номера соцстрахования).

Помимо кражи информации с ее последующей продажей, также следует обратить внимание на атаки с шифровальщиками, причиняющие своим жертвам прямой экономический ущерб. Больницы, фармацевтические и страховые компании имеют огромный объем ценной информации. Кибер-преступники обратили на них свое пристальное внимание. Они постоянно ищут новые возможности для доступа к этой информации.

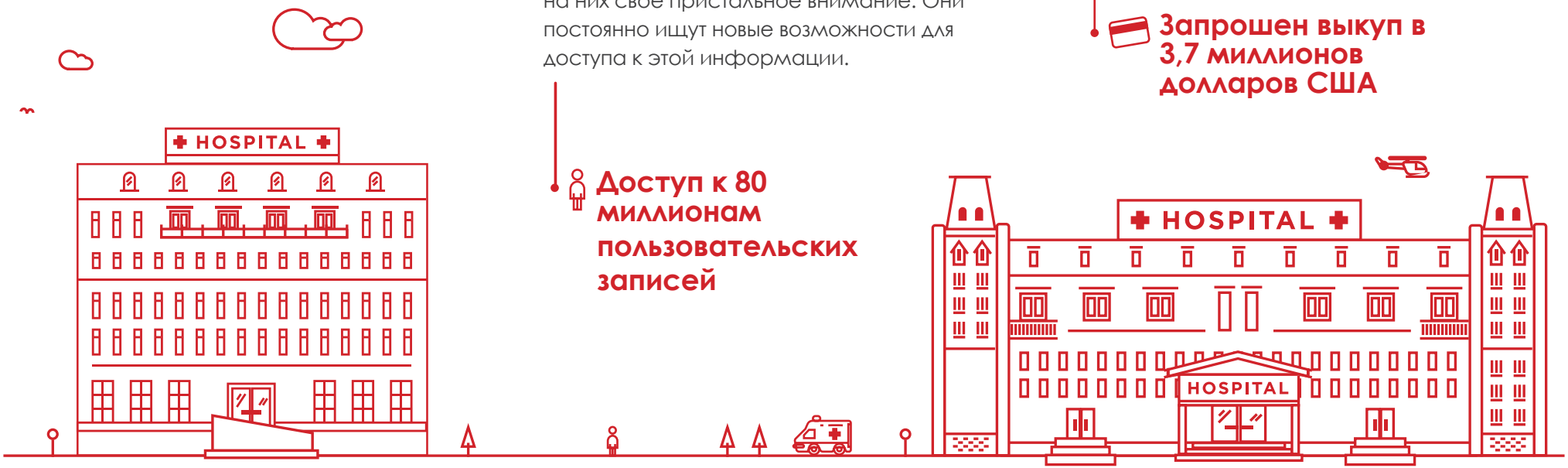
Пресвитерианский медицинский центр в Голливуде (США)

В феврале 2016 году Пресвитерианский медицинский центр в Голливуде (Лос-Анджелес, США) объявил "внутреннюю опасность", т.к. их сотрудники остались без доступа к медицинским записям пациентов, электронной почты и других систем.

В результате некоторые пациенты не смогли получить должное лечение и были отправлены в другие больницы. Кибер-преступники потребовали выкуп в размере 3,7 миллионов долларов США. В итоге Руководитель центра договорился с ними и заплатил примерно 17 тысяч долларов, чтобы получить похищенные файлы.

Запрошен выкуп в 3,7 миллионов долларов США

Доступ к 80 миллионам пользовательских записей



Baltimore MedStar Health (США)

В следующем месяце MedStar Health из Балтимора (США) также признались, что они были вынуждены отключить некоторые системы своей больницы в результате подобной атаки.

Они вынуждены были отключить системы своей больницы

Госпиталь Henderson Metthodist (США)

Больница в Хендерсоне (Кентукки, США) стала еще одной жертвой.

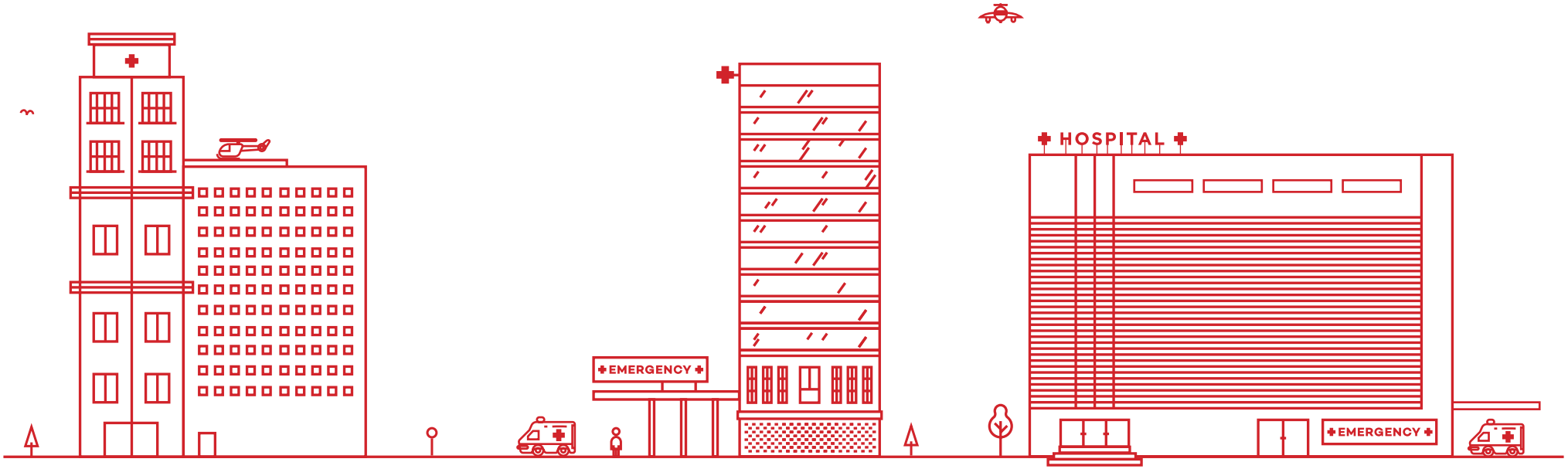
В этом случае есть неподтвержденная информация, что был заплачен выкуп в 17000 долларов США, хотя предполагается, что реально было заплачено намного больше.

Заплачено 17000 долларов США

Prime Healthcare Management

Крупный провайдер медуслуг в США, Prime Healthcare Management, Inc., также стал жертвой кибер-атак. Были атакованы две их больницы (Chinese Valley Medical Center и Desert Valley Hospital), вызвав отключения сети, и многие другие объекты, пострадавшие от этой же атаки. В данном случае компания не платила выкуп.

Две их больницы были атакованы



Случаи в Германии

Больницы США - не единственные цели: жертвами атак были и немецкие больницы.

По данным международной телерадиокомпании Deutsche Welle, несколько больниц в Германии пострадали от шифровальщиков, среди них - Lukas Hospital в Нойсе и Klinikum Arnsberg в Северном Рейне-Вестфалии. Никто из них не платил выкуп.

Были атакованы несколько больниц в Германии

Кардиологическая больница в Канзасе (США)

Следует отметить, что выплата выкупа в примерах выше не гарантировала возврата информации. Ярким примером этого является атака шифровальщика на кардиологическую больницу в Канзасе (США) в мае 2016 года. Руководитель больницы решил заплатить выкуп, но хакеры, осознав ценность данных, запросили еще денег за восстановление оставшейся информации. Больница не стала делать второй платеж.

Хакеры запросили второй платеж

"Профилактика лучше лечения"

Все эти случаи наглядно показывают, что сектору здравоохранения следует прислушаться к своему собственному совету.

Реальность научной фантастики

Как показано в примерах выше, эти типы атак в полной мере способны остановить работу больницы, закрыв доступ к файлам и взяв в заложники чувствительную информацию.

Кроме этого, есть нечто, что может серьезно повлиять на каждого из нас. Практически все медицинское оборудование (например, кардиостимуляторы, томографы, рентгены, инфузионные насосы, респираторы и т.д.) подключено к сети . Вполне реально, что эти медицинские устройства могут быть взломаны.

В 2013 году бывший вице-президент США Дик Чейни сообщил, что его врачи отключили беспроводную связь с его кардиостимулятором, потому что они увидели, что высока вероятность удаленной атаки на его устройство.

Годом ранее Барнаби Джэк, хакер из Новой Зеландии, продемонстрировал участникам конференции по безопасности, как **удаленно может быть взломан кардиостимулятор, который привел к опасному для жизни электрошоку**. Барнаби придумал атаку, которая могла бы поразить все кардиостимуляторы в радиусе 15 метров.

Он также показал, как можно на расстоянии до 90 метров удаленно изменить параметры работы портативной инсулиновой помпы, используемой больными диабетом, в результате чего она может впрыснуть пациенту летальную дозу инсулина.

Джэк умер за неделю до того, как он был готов продемонстрировать взлом искусственного сердца. На конференции Black Hat Conference 2013 он бы показал, как можно менять параметры работы этих имплантатов.

Барнаби Джек

Показал, как удаленно можно менять параметры работы многих медицинских устройств.

Ричард Риос

Выявил свыше 300 уязвимых устройств в 40 различных компаниях.

Ричард Риос также посвятил себя поиску уязвимостей в медицинских приборах. Из-за полипа в его дыхательных путях этот исследователь оказался на две недели в Стэнфордском госпитале. За это время Риос понял, что его кровать подключена к компьютеру. На ней были пояса, которые поднимали его ноги, и инфузионный насос, который ежедневно вводил лекарства. Не покидая палаты, он исследовал и нашел до 16 сетей и 8 точек доступа Wi-Fi.

Пролежав в постели несколько дней, он встал и пошел к выходу, чтобы размять свои ноги. За время этой небольшой прогулки он обнаружил компьютеризованный дозатор препаратов. Вся ответственность за распространение лекарств целиком лежала на компьютере, которым управляли доктор и медсестры, используя закодированную идентификационную карту. Прежде, чем заметив прибор, Ричард уже понял, что эта система имеет уязвимости: пароль, жестко встроенный в исходный код программы, позволял другим "играть" с дозатором лекарств.

Вместе со своим напарником Терри МакКорклом, Ричард обнаружил свыше 300 уязвимых устройств в 40 компаниях в сфере здравоохранения. Риос уверен, что эти уязвимости существуют до сих пор.

В своем рвении продемонстрировать опасность этих уязвимостей, **Ричард Риос сумел показать, что можно удаленно манипулировать медицинскими помпами,** используемыми в больницах всего мира.

Он взломал несколько таких устройств, чтобы повысить уровень доз до смертельно опасных значений. Риос предупредил, что такое можно проделать на более чем 400 000 таких помп во всем мире, которые остаются уязвимы.

Почти одновременно с ним, несколько аналитиков из TrapX Security (Сан-Матео, Калифорния, США) начали отслеживать уязвимые устройства в более чем 60 больницах. **Они заразили сотни устройств с помощью программы, которая заменила часть оригинальной операционной системы на данных устройствах.** Зараженные машины оставались полностью работоспособны, поэтому никто не заметил проблемы, но за эти 6 месяцев TrapX отследил всю работу сетей этих больниц.

Среди устройств, к которым они получили доступ, были также рентгеновские аппараты, аппараты для анализа крови, помпы, и, конечно же, компьютеры, используемые сотрудниками больниц. Многие такие компьютеры имели неподдерживаемые операционные системы, которые являются более уязвимыми, такие как Windows XP или Windows 2000.

Тот факт, что антивирусная защита большинства этих больниц не обнаружила внедрение TrapX, говорит о том, что их устройства недостаточно хорошо защищены. Они оставались зараженными до тех пор, пока TrapX Security не стал бить тревогу.

Как можно было бы избежать этих атак?

Мы видели, как преступники осуществляют атаки для кражи чувствительной информации, истории болезней, фармацевтические исследования или данные страхователей. Мы видели, как они без проблем узнают адреса электронной почты, пароли и номера соцстраховок. Или как шифровальщики, чтобы заработать деньги, крадут важную информацию, которая может парализовать работу все больницы.

Избежать этих атак - задача сложная. Но необходимо осуществлять конкретные действия: выделить ресурсы и разработать политики для повышения уровня безопасности устройств, данных и людей.

Первая основная и решающая рекомендация: **использовать решение ИТ-безопасности с возможностями расширенной защиты, которая может обнаруживать и устранять возможные угрозы**.

Многие атаки были успешны благодаря недостатку контроля над всем, что происходит в компьютерных системах. Мы рекомендуем использовать модель, способную контролировать все активные процессы на устройствах, подключенных к корпоративной сети.

Имея полную видимость того, что происходит, можно контролировать любое аномальное поведение в системах и действовать прежде, чем возникнет какой-либо инцидент.

Кроме того, компаниям, которые обрабатывают чувствительную информацию, следует **проверить свою кадровую политику и контролировать системы, чтобы обеспечить выполнение требований конфиденциальности и адаптироваться к доступным технологиям**.

Наш последний совет, о котором мы часто говорим и который проще, чем кажется, но редко выполняется: **всегда необходимо регулярно обновлять операционные системы и программы**. Таким образом, будет закрыто большинство известных уязвимостей благодаря корректирующим патчам, которые выпускаются производителем.

Хорошо иметь политику обновлений и контроль доступных устройств. Такой тип системы управления предлагает инструменты мониторинга и инвентаризации, что поможет сделать ИТ-хозяйство более эффективным, единым, централизованным и безопасным.

Решение

Для защиты от современных угроз и целенаправленных атак мы должны иметь систему, которая обеспечивает конфиденциальность информации, защиту данных, деловой репутации и ИТ-активов.

Adaptive Defense 360 **- это первый и единственный сервис информационной безопасности, который сочетает в себе один из самых эффективных традиционных антивирусов с самой современной защитой и возможности классификации всех исполняемых процессов**.

Adaptive Defensive 360 способен обнаруживать вредоносные программы и странное поведение, которые не обнаруживаются другими сервисами защиты, за счет классификации всех запущенных и исполняемых процессов.

Благодаря этому решение способно обеспечивать защиту от известных вредоносных программ, а также от атак "нулевого дня", постоянных угроз повышенной сложности (Advanced Persistent Threats, APT) и целенаправленных атак.

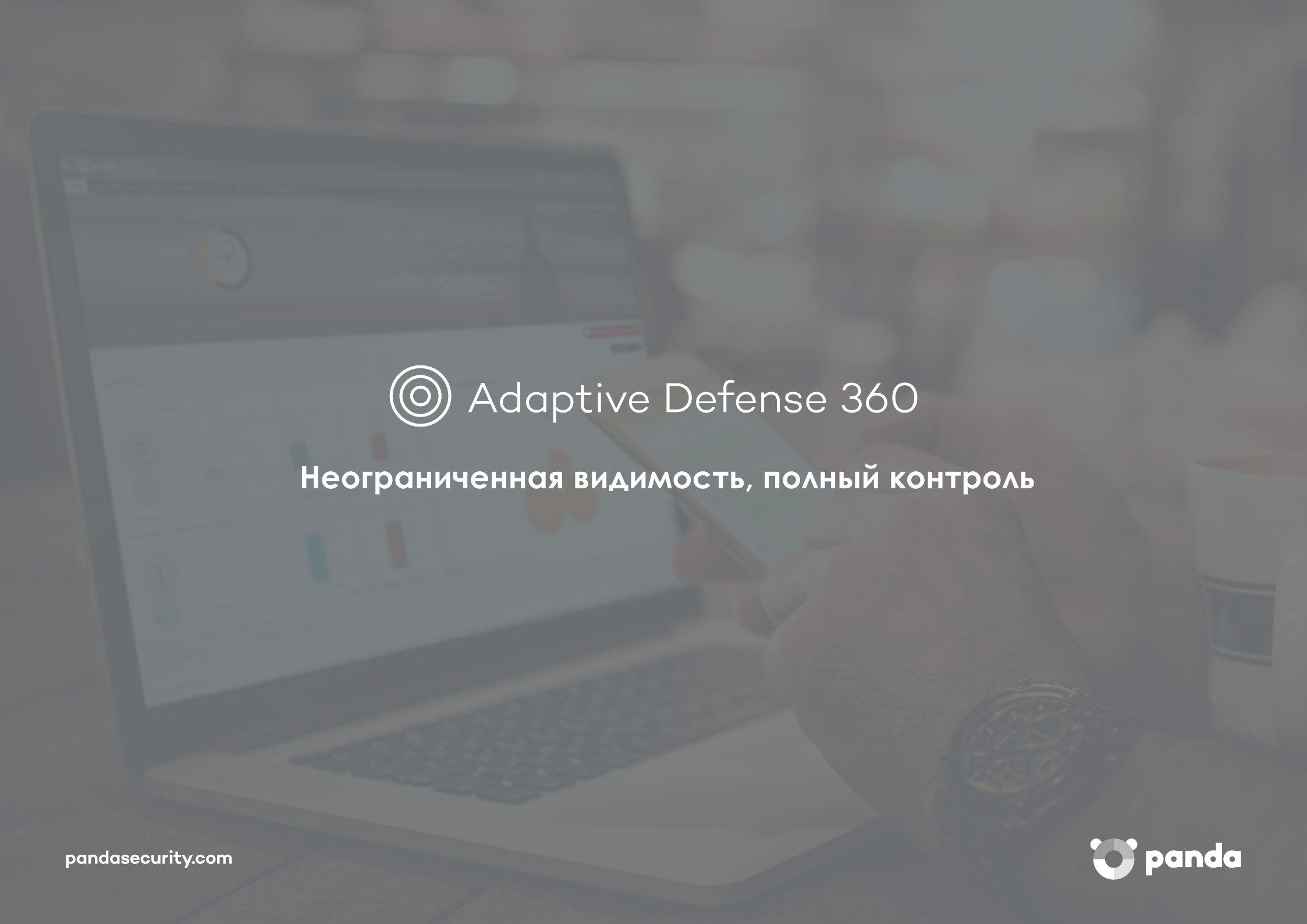
С помощью Adaptive Defense 360 Вы всегда будете знать, что происходит с каждым Вашим файлом и процессом.

Подробные графики показывают все, что происходит в сети: хронология угроз, поток информации, как ведут себя активные процессы, как вредоносные программы проникают в систему, где это происходит, с кем, как угрозы получают доступ к информации и т.д.

Adaptive Defense 360 позволяет легко обнаруживать и закрывать уязвимости, а также предотвращать нежелательные элементы (навигационные тулбары, рекламное ПО, дополнительные компоненты и пр.).

Adaptive Defense 360: неограниченная видимость, полный контроль.

Подробнее:
pandasecurity.com/russia/enterprise/solutions/adaptive-defense-360/



Adaptive Defense 360

Неограниченная видимость, полный контроль

pandasecurity.com

panda

Подробная информация:

pandasecurity.com/russia/enterprise/solutions/adaptive-defense-360/

По телефону:

+7 495 105 94 51

или по почте sales@rus.pandasecurity.com

panda