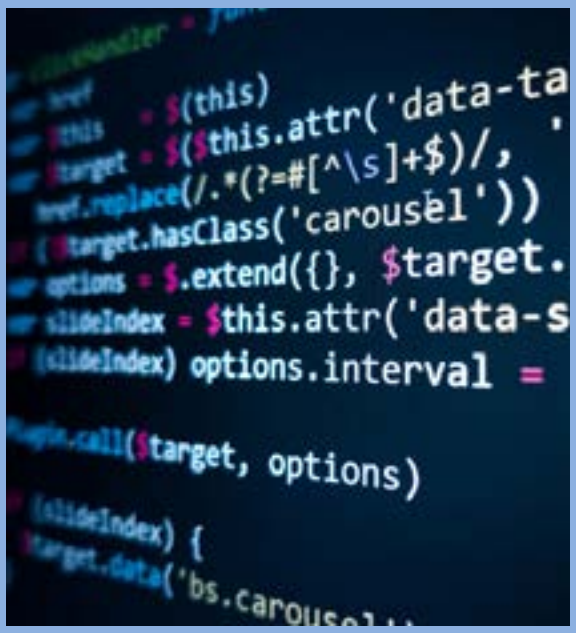
SPINETIX™
N°1 IN DIGITAL SIGNAGE SOLUTIONS

Цена информационной безопасности в Digital Signage

За последние два года произошло несколько крупных кибератак. Самые известные — WannaCry и NotPetya. Также были обнаружены аппаратные уязвимости безопасности, например, Meltdown и Spectre.

Вредоносные программы WannaCry и NotPetya вызвали серьезные сбои в работе IT служб и нанесли серьезный ущерб. Вирусы блокировали работу организаций во всем мире: учреждений здравоохранения, аэропортов, банков, заводов, предприятий малого бизнеса. Пострадало много частных лиц. В некоторых случаях потребовалось несколько дней для полного восстановления работоспособности систем.

Уязвимость Meltdown имеет поражающие масштабы. Эта аппаратная уязвимость обнаружена почти во всех микропроцессорах, выпущенных с 1995 года. Благодаря своевременному обнаружению Meltdown, эта уязвимость ни разу не использовалась для кибератак.

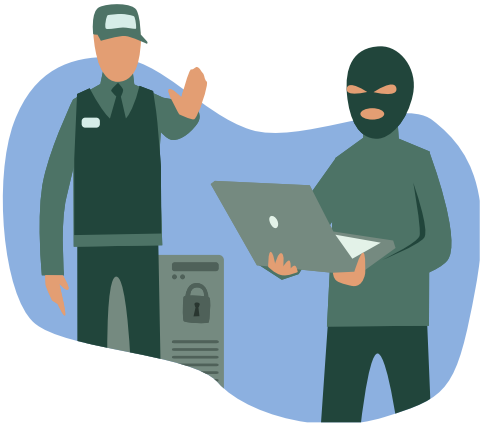


Кроме масштабных и известных кибератак, было много случаев узкопрофильных и специфичных для индустрии digital signage вредоносных действий. От относительно лояльных сообщений «Проверьте безопасность вашей системы» до трансляции порно в общественных местах.

Информационная безопасность — основное требование к инсталляции Digital Signage

С увеличением числа систем Digital Signage, количество атак будет неуклонно расти. Критически важно рассматривать вопросы безопасности в качестве основного требования при планировании, развертывании и эксплуатации решений Digital Signage. К сожалению, при выборе продуктов для нового проекта, аспект безопасности чаще всего игнорируется. Основными критериями являются закупочная стоимость, эксплуатационные расходы, технические характеристики и производительность.

Вопросы безопасности digital signage часто не принимаются всерьез, что в конечном счете приводит к неприятным последствиям. Информационная безопасность должна быть в приоритете абсолютно для всех сторон — и маркетинга, и IT.



Лица, принимающие решения, часто ошибочно предполагают одинаковую безопасность решений разных поставщиков. Надеются, что шансы злоумышленников воспользоваться уязвимостью малы, а ущерб — несерьезен. Ни одно из этих утверждений в настоящее время не имеет силы в реальном мире.

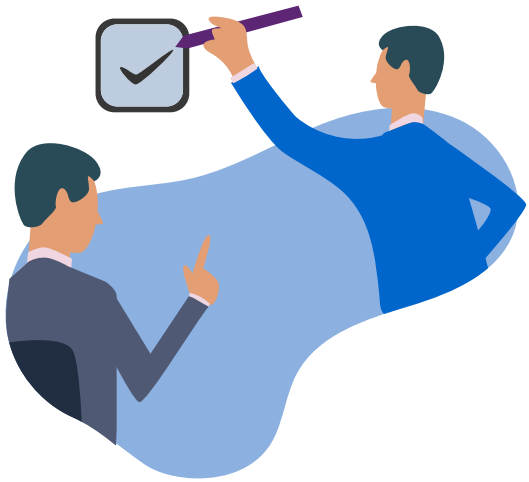
Риск кибератаки как никогда реален и не обходится без серьезных последствий. Взлом системы безопасности может привести к простоям, потерям от рекламных доходов и даже потере имиджа вашей компании. Скомпрометированная установка Digital Signage может также быть использована для атаки на другие ИТ-инфраструктуры.

Без активных действий программное обеспечение не может оставаться защищенным. Любое ПО всегда имеет неизвестные уязвимости. Важно, чтобы они были своевременно устранены.

Проект digital signage: что принимать во внимание при оценке безопасности.

Сеть digital signage состоит из нескольких объектов. Слабые стороны есть у каждого звена. Например, надо анализировать безопасность физического доступа к панелям и плеерам, размещенным в публичных местах. Иначе злоумышленник может физически подменить источник сигнала. Надо оценивать безопасность медиаплеера, дисплея, защищенность сети, каналов передачи данных, источников данных, уязвимость скриптов, контент.

Все перечисленное надо учитывать в момент выбора оборудования. Поздняя интеграция элементов безопасности зачастую невозможна, либо очень дорого стоит.



Вопросы, на которые следует ответить при выборе компонентов digital signage:

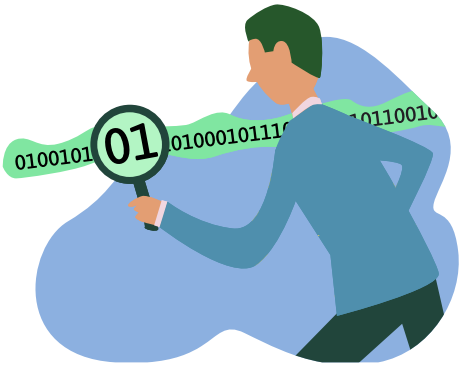
- Удовлетворительная ли у поставщика репутация на рынке?
- Референсы поставщика по выполненным инсталляциям?
- Выполняет ли поставщик регулярные обновления безопасности?
- Какой срок обслуживания поставляемого продукта?
- Прозрачна ли информация о конкретных исправленных проблемах в каждом обновлении?
- Как делаются обновления и как дорого обходится их выполнение?
- Есть ли обратная совместимость обновлений?
- Насколько квалифицирована служба технической поддержки?

Эти вопросы помогают понять, поддерживает ли производитель безопасность продукта, и насколько сложно выполнять обновления.

Кроме вопросов безопасности самих устройств, необходимо учитывать безопасость для цепочки производства, приобретения и дистрибуции контента. Каким образом контент передается на плеер? Когда контент извлекается плеером, например, из социальных сетей, безопасно ли это? Существует ли необходимость хранения на устройстве паролей в виде открытого текста для подключения к каналам социальных сетей или другим внешним ресурсам? Если хранить пароли необходимо, защищены ли они от несанкционированного доступа?

Цена безопасности.

Выполнить требования безопасности и поддерживать ее на должном уровне — дорого. Обнаружение уязвимостей, мониторинг ресурсов по безопасности, создание защищенных решений — длительный каждодневный процесс. Поддержка системы digital signage в актуальном безопасном состоянии в момент, когда продукт находится уже у клиента — вдвойне сложная задача.



Защищенное решение стоит дороже.

На первый взгляд может показаться, что для обеспечения информационной безопасности, нужно принять во внимание слишком многое. Это не так. Если рассматривать вопросы безопасности с самого начала проекта и учитывать данные критерии при выборе поставщика, все становится прозрачным. Выбирайте поставщика любых частей системы digital signage с репутацией и историей, опытом инсталляций, удобными инструментами установки критических обновлений системы, локальной техподдержкой, и специально созданной службой обеспечения безопасности.

Диего Санта Круз,
Кандидат технических наук, архитектор технологий SpinetiX

Несколько слов об авторе

Диего занимается безопасностью продуктов SpinetiX более 10 лет. Он является соучредителем SpinetiX и отвечает за вопросы развития системного уровня. Ежедневно от 2 до 4 часов Диего и его подчиненные тратят на изучение сводок по уязвимостям, анализ существующих и вероятных опасностей, разрабатывают решения для защиты продуктов SpinetiX.

Специализация Диего — разработка систем и ядер, сетевые протоколы, безопасность, IT и электроника, системы отображения, видео. Диего получил докторскую степень в области видеообработки, и является одним из ранних последователей Linux. Диего автор нескольких патентов на изобретения, и участник комитетов, разрабатывавших JPEG и