Безопасное использование WEB-Технологий, web-ресурсов и порталов органов государственной власти

Немошкалов Александр
Директор по развитию бизнеса

ЦИФРОВАЯ ЭКОНОМИКА

…хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг.

- создание условий для развития общества знаний в РФ;
- повышение благосостояния и качества жизни граждан путем повышения доступности и качества товаров и услуг, произведенных в цифровой экономике с использованием современных цифровых технологий;
- повышение степени информированности и цифровой грамотности населения;
- улучшение доступности и качества государственных услуг для граждан;
- обеспечение информационной безопасности как внутри страны, так и за ее пределами

СЛЕДУЕТ УЧЕСТЬ

ГОСУДАРСТВО

БИЗНЕС

ГРАЖДАНЕ

Инфраструктура взаимодействия между трем классами разношерстна – нет унификации, что приводит к значительным сложностям при обеспечении безопасности коммуникаций внутри государства.

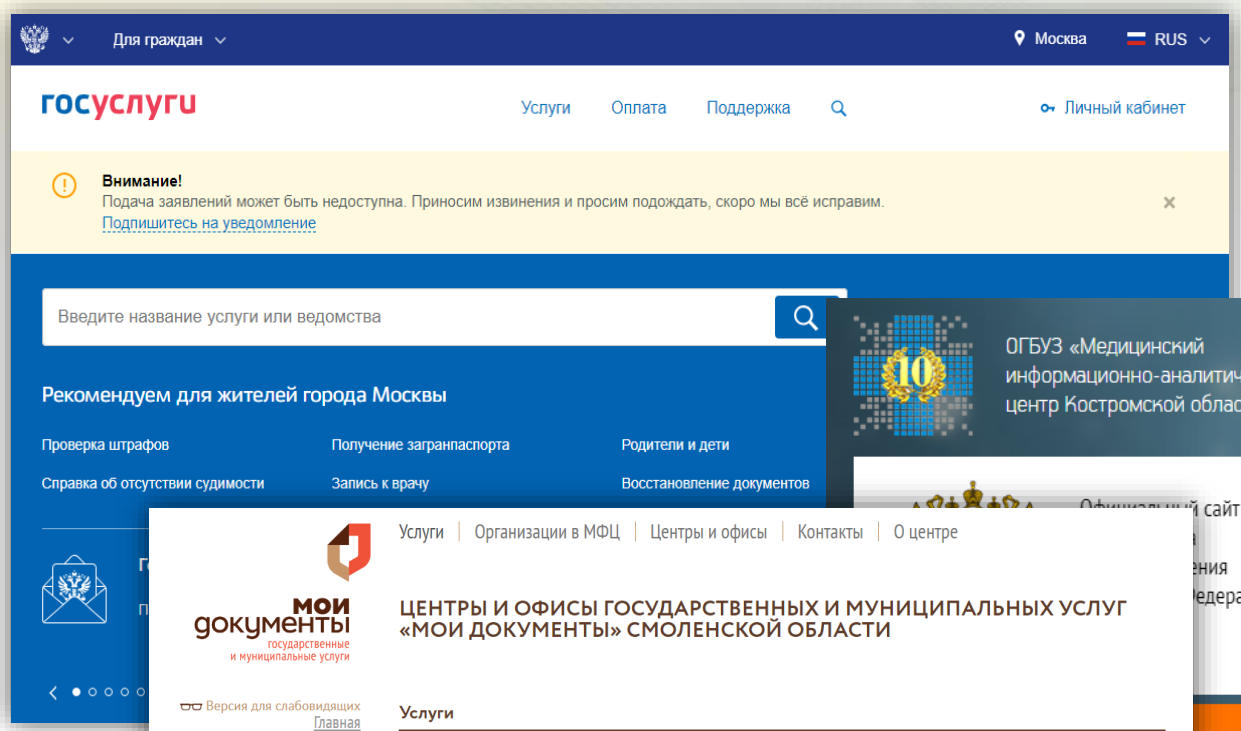
Понимание потребности в решениях по информационной безопасности для минимизации рисков, связанных применением информационных технологий как на пользовательском, так и на корпоративном уровне не на должном уровне.

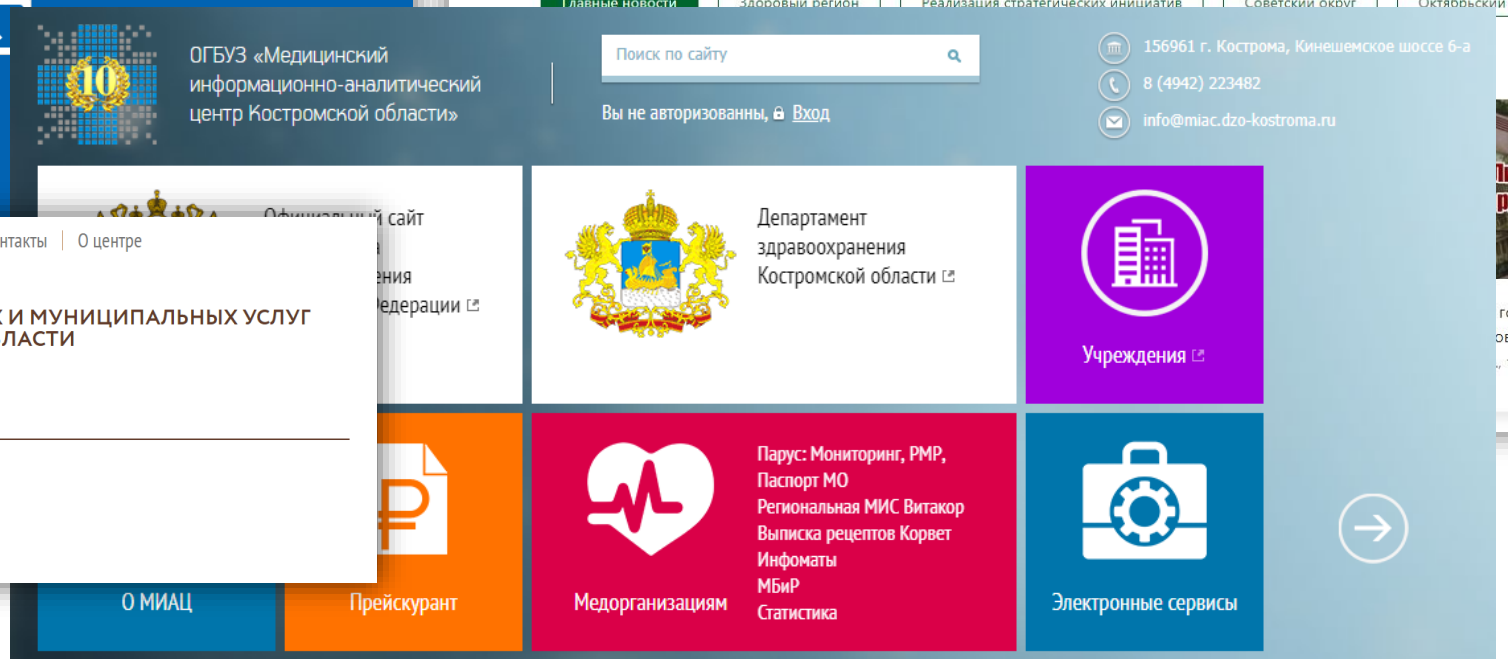
Качество отечественных средств защиты, призванных обезопасить все бизнес-процессы, социальные и государственные процессы, как правило уступает западным аналогам. Пока уступает…

Отсутствие финансирования, либо понимания в необходимости финансирования проектов, связанных с защитой активов, информационных систем, данных – еще одна из задач, которую необходимо решить.

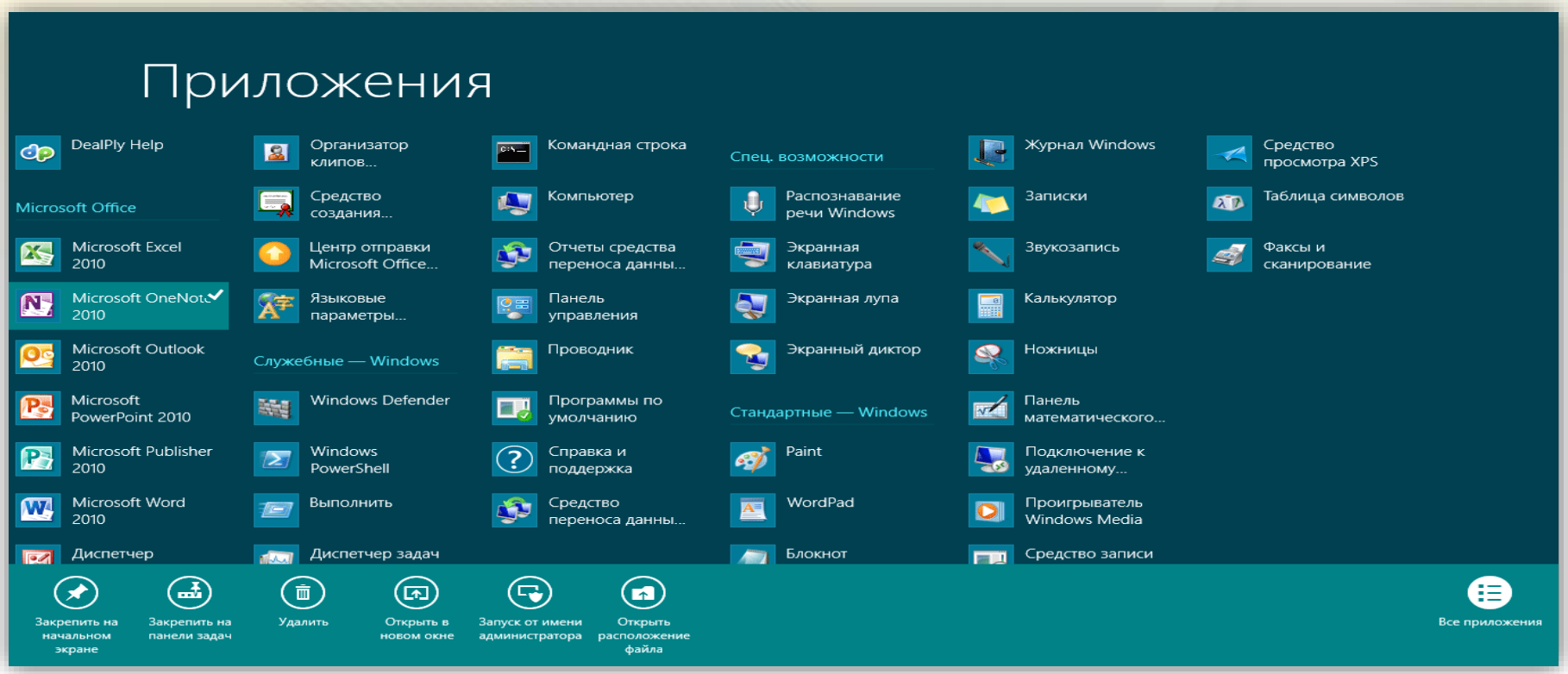
КОД БЕЗОПАСНОСТИ

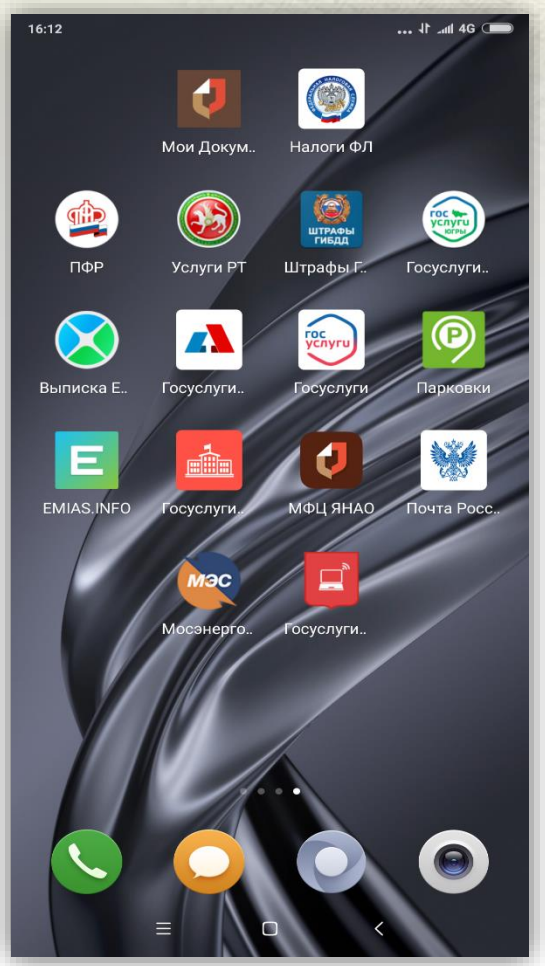
ПРЕДМЕТ ДЛЯ БЕСЕДЫ





ПРИЛОЖЕНИЯ КАК СУТЬ





Веб-приложение — клиент-серверное приложение, в котором клиент взаимодействует с сервером при помощи браузера, а за сервер отвечает — веб-сервер.

Логика веб-приложения распределена между сервером и клиентом, хранение данных осуществляется, преимущественно, на сервере, обмен информацией происходит по сети.

Одним из преимуществ такого подхода является тот факт, что клиенты не зависят от конкретной операционной системы пользователя, поэтому веб-приложения являются межплатформенными службами.

ПРОБЛЕМАТИКА

В первую очередь атака несет угрозу работоспособности сайта. Во вторую, но не менее важную, — сохранность пользовательских данных. Из этих причин вытекает логичное следствие — финансовые и репутационные потери компании.

Хакеры используют ваш сайт для атак на другие ресурсы, в качестве опорного плацдарма, для рассылки спама или проведения DoS атак. Ваш сайт блокируют поисковики и браузеры, вы теряете пользователей.

Атака на веб-сайт в корпоративной среде может является т.н. точкой входа в корпоративную сеть компании.

Атаки на системы электронной коммерции могут быть использованы для совершения мошеннических действий, похищения клиентских баз и т.д.

ПРОБЛЕМАТИКА

Природа атак

Распространение атак на веб-приложения связаны с двумя основными факторами: халатное отношение к безопасности сайта и низкий порог входа потенциальных злоумышленников.

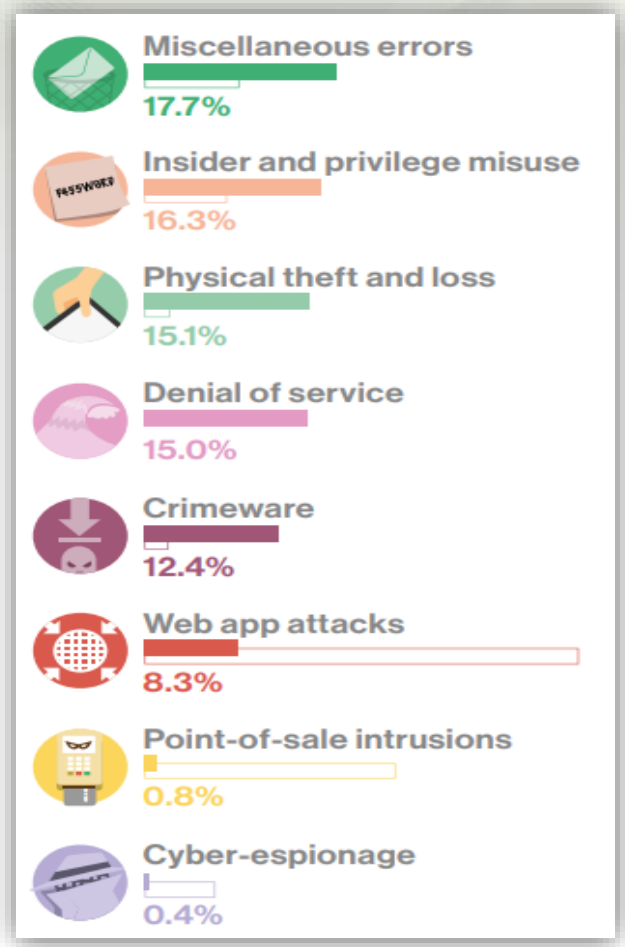
В большинстве случаев на сайтах не используются специальные средства обнаружения, мониторинга и защиты, а также нет ответственного персонала и осведомленности об угрозах безопасности сайта. Качеству кода и безопасной настройке веб-приложения (и веб-сервера) уделяется мало внимания.

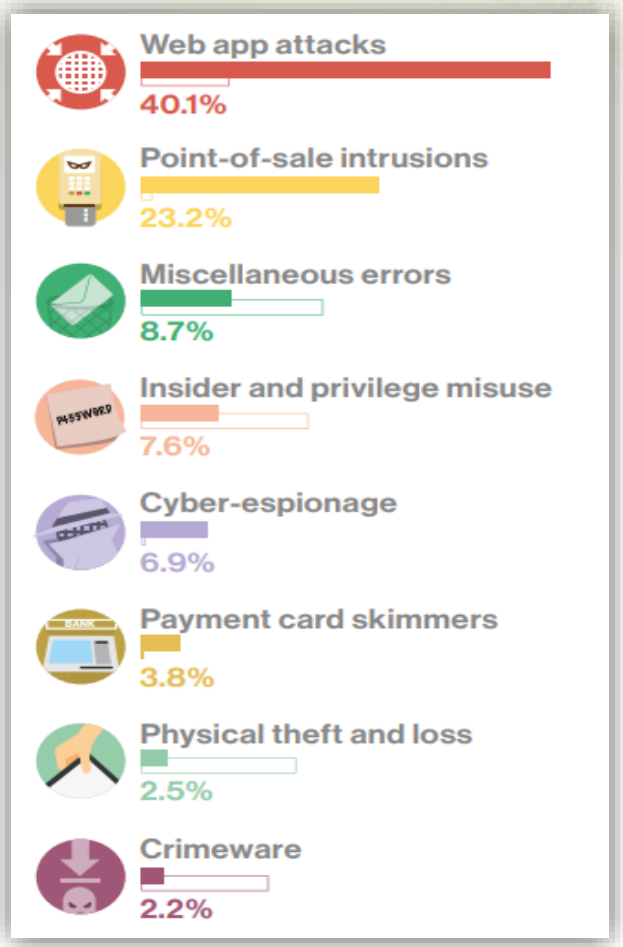
МЕЖДУНАРОДНЫЙ ОПЫТ

2016 Data Breach Investigations Report

Executive Summary

verizon



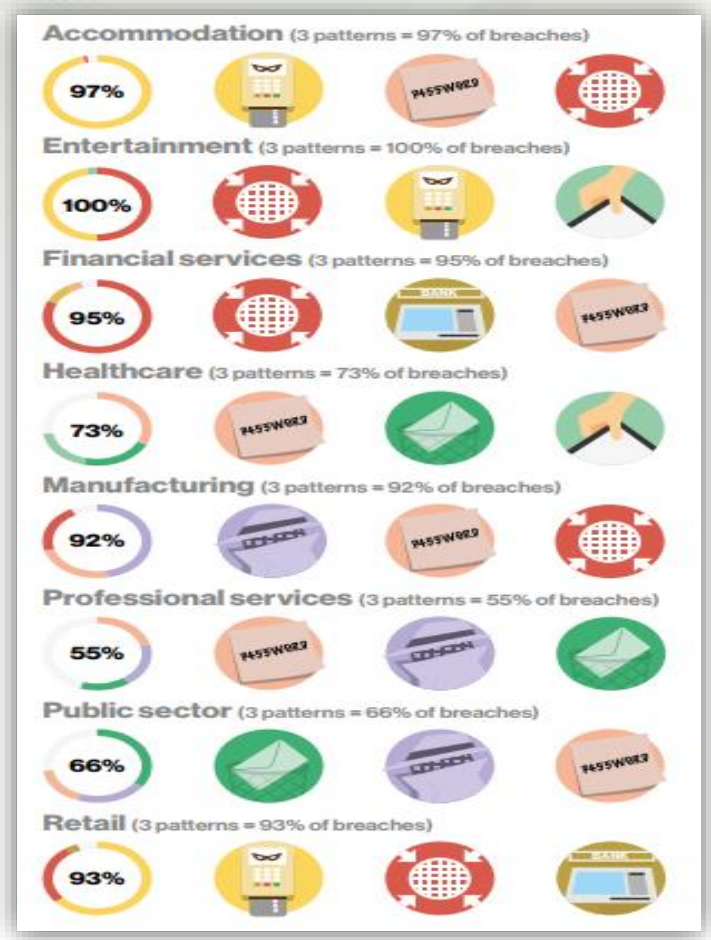


МЕЖДУНАРОДНЫЙ ОПЫТ

2016 Data Breach Investigations Report

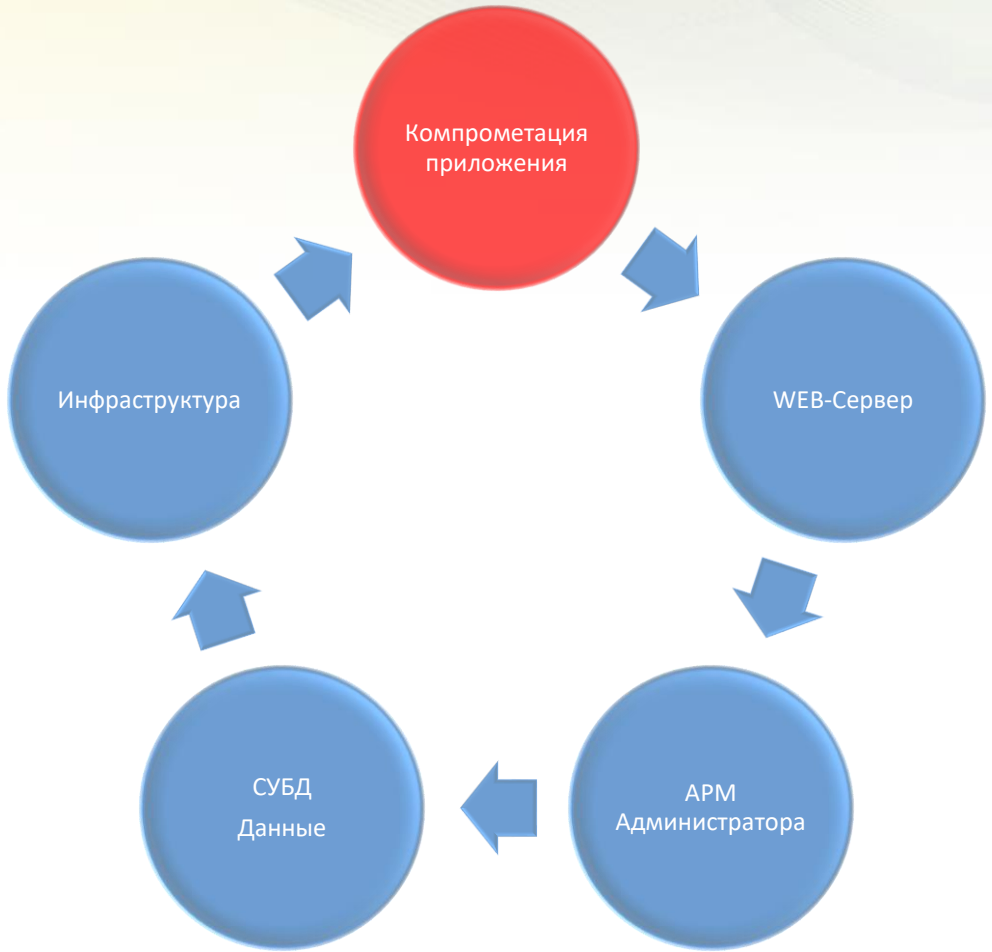
Executive Summary

verizon



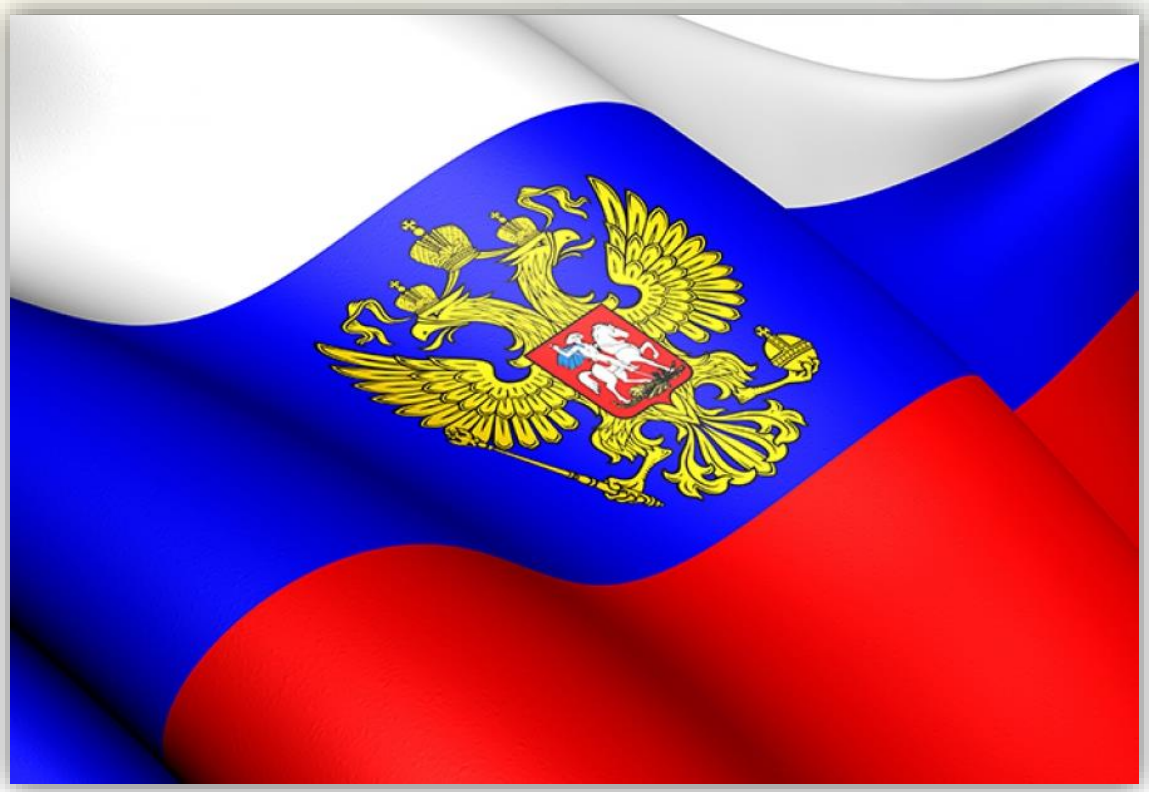
В рамках данного отчёта основными отраслями для атак через веб-приложения являются ритейл, финансовые блоки, производственные организации, компании, оказывающие услуги в области развлечений, ЖКХ и организации, осуществляющие деятельность с недвижимостью.

К ЧЕМУ ЭТО ПРИВОДИТ



Компрометация приложений – это достаточно лёгкий процесс. Но он приводит к очень серьезным последствиям для функционального заказчика. Мы констатируем факт того, что сами приложения – это лишь первый шаг для достижения целей злоумышленников. Дальнейшие шаги будут направлены на проникновение в инфраструктуру заказчика, компрометацию администратора и управляемых модулей, кражу данных и вывод инфраструктуры из строя.

ГИС



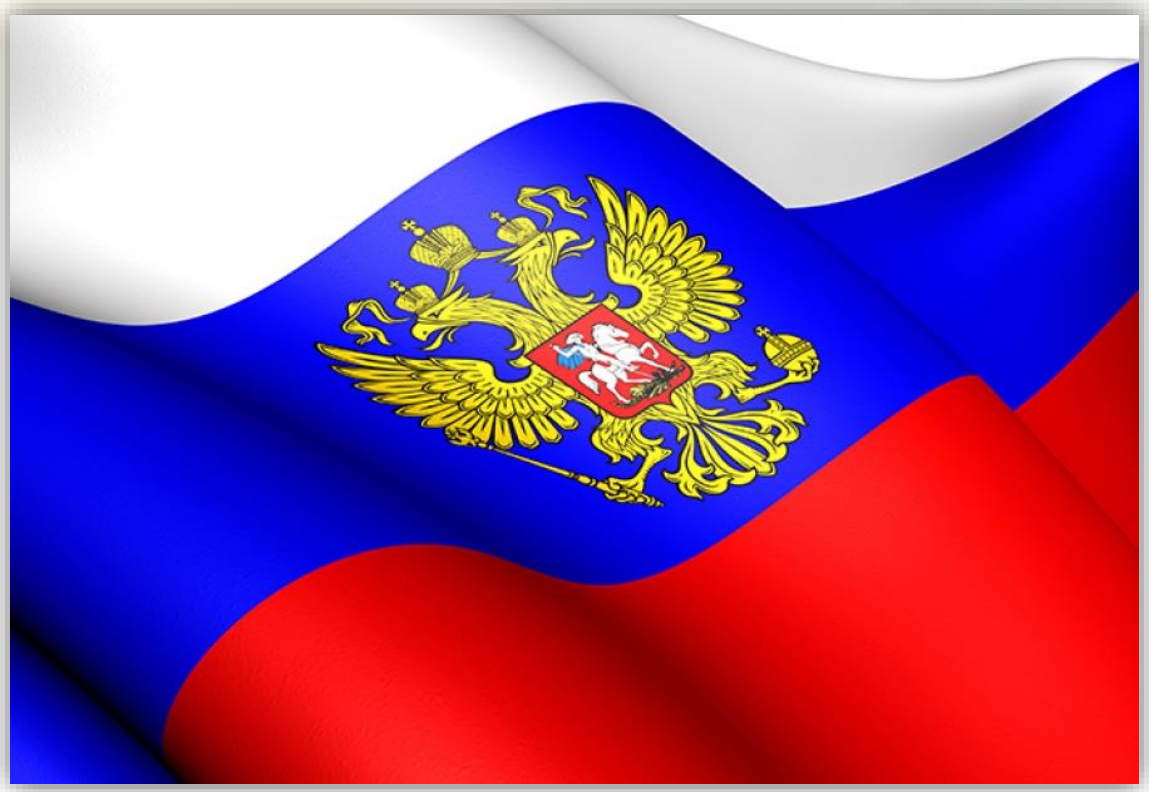
Публичные федеральные и региональные информационные ресурсы (сайты министерств, ведомств, должностных лиц)

Федеральные и региональные системы (порталы) предоставления государственных услуг

Системы межведомственного взаимодействия

Территориально-распределенные системы внутриведомственного взаимодействия

ВОЗМОЖНЫЕ АТАКИ НА ГИС



Атаки на отказ в обслуживании

Намеренное изменение содержимого веб-страниц сайта

Атаки, направленные на пользователей веб-ресурса

Мошеннические манипуляции с веб-ресурсом

Атаки на внутренние ресурсы организации

Несанкционированные действия внутреннего нарушителя

КОД БЕЗОПАСНОСТИ

МЫ РЕШАЕМ СЛЕДУЮЩИЕ ЗАДАЧИ

ЗАЩИТА ПЕРИМЕТРА СЕТИ

СОЗДАНИЕ VPN-СЕТЕЙ НА ОТЕЧЕСТВЕННЫХ КРИПТОАЛГОРИТМАХ – L2/L3

ПРОАКТИВНАЯ ЗАЩИТА ПЕРИМЕТРА СЕТИ ПРИ ПОМОЩИ СИСТЕМ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ WEB-ПЛАТФОРМ

ЗАЩИТА WEB-ПОРТАЛОВ И ДОСТУПА К НИМ ЗА СЧЁТ ПРИМЕНЕНИЯ WAF И TLS

КОРПОРАТИВНЫЕ МЕЖСЕТЕВЫЕ ЭКРАНЫ НОВОГО ПОКОЛЕНИЯ – NGFW

ЗАЩИТА ДАННЫХ И ДОСТУПА К НИМ

КОНТРОЛЬ И ЗАЩИТА СРЕДЫ ВИРТУАЛИЗАЦИИ

МНОГОУРОВНЕВАЯ СИСТЕМА ЗАЩИТЫ ДАННЫХ НА АРМ И СЕРВЕРАХ С ПРИМЕНЕНИЕМ ФУНКЦИОНАЛА СЗИ от НСД, СОВ, АПМДЗ, СОЗДАНИЯ ДОВЕРЕННОЙ СРЕДЫ, АНТИВИРУСНОЙ ЗАЩИТЫ, КОНТРОЛЯ ПРИМЕНЕНИЯ ОТЧУЖДАЕМЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ И МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ В ПРЕДЕЛАХ ЛВС

АДМИНИСТРИРОВАНИЕ И КОНТРОЛЬ ПРИМЕНЯЕМЫХ В КОРПОРАТИВНОЙ СРЕДЕ МОБИЛЬНЫХ УСТРОЙСТВ И ДЕВАЙСОВ

КОД БЕЗОПАСНОСТИ

ПРЕДМЕТНО!

КОНТИНЕНТ TLS

Система обеспечения защищенного удаленного доступа к веб-приложениям с использованием алгоритмов шифрования ГОСТ

КОНТИНЕНТ WAF

Система защиты веб-приложений и автоматизированный анализ их бизнес-логики

КОНТИНЕНТ IPS

Высокопроизводительная система обнаружения и предотвращения вторжений с иерархическим управлением и возможностью контроля сетевых приложений

БЛАГОДАРЮ ЗА ВНИМАНИЕ!

Немошкалов Александр

a.nemoshkalov@securitycode.ru
+7 (495) 982 30 20 (*495)
+7 916 082 85 73