WEBTOTEM

Результаты анализа защищенности веб-ресурсов государственных организаций Республики Казахстан (2020)

WEBTOTEM.AI

Содержание

Глоссарий

Информационная безопасность

Сохранение конфиденциальности, целостности и доступности информации;

Уязвимость

Недостаток программного средства или информационной системы, который может быть использован для реализации угроз безопасности информации, с целью намеренно нарушить работу и целостность программного средства или информационной системы.

Риск

Это потенциальная возможность использования уязвимостей программного обеспечения или информационной системы, с целью нанесения ущерба организации.

Угроза

Совокупность возможных факторов, которые могут привести к нарушению и причинению вреда информационной безопасности организации.

Атака

Попытка уничтожить, раскрыть, изменить, сделать недоступным, украсть или получить несанкционированный доступ или не санкционированно использовать актив.

Введение

Сегодня государственным органам доверено беспрецедентное количество конфиденциальных данных. Ставки очень высоки: взлом государственных веб-сервисов ставит под угрозу национальную безопасность, защиту персональных данных граждан, а также доверие казахстанцев к государству. Кибербезопасность является одним из основных препятствий на пути цифровой трансформации.
Содействуя концепции кибербезопасности "Киберщит Казахстана", утвержденной постановлением Правительства Республики Казахстан (далее – РК) от 30 июня 2017 года №407, продукт собственной разработки Центра анализа и расследования кибер-атак (далее - ЦАРКА) WebTotem AI на постоянной основе ведет мониторинг защищенности сайтов казнета.

Отчет был подготовлен ЦАРКА по результатам тестирования веб-ресурсов госорганизаций РК, проведенного в ноябре 2020 года продуктом собственной разработки WebTotem AI.
Система WebTotem AI основана на алгоритме искусственного интеллекта, который позволяет выявлять уязвимости и угрозы в киберпространстве.

ЦАРКА искренне надеется, что проделанная работа поможет отделам информационной безопасности госорганизаций обратить внимание на выявленные уязвимости, которые потенциально могут быть использованы злоумышленниками, а также будет способствовать повышению уровня защиты в соответствии с лучшими мировыми практиками.

Цель исследования

Основной целью данного исследования было выяснить, как государственные организации РК обеспечивают безопасность своих веб-ресурсов. Оценка уровня безопасности проводилась в соответствии с лучшими практиками в области информационной безопасности такими как OWASP Топ-10, ISO 27001-2013.

Метод исследования

Эксперты ЦАРКА использовали неинвазивные методы сканирования, изучая основной домен госорганизации, его главную страницу и почтовый сервер. Тестирование проводилось без нарушения функционирования веб-ресурсов, по средствам отправки «легких» HTTP и DNS-запросов и анализа ответов с сервера. Работа включала в себя анализ практик и рекомендаций для настроек веб-серверов.
Были выбраны ключевые точки контроля, которые можно проверить не вмешиваясь в основную работу веб-ресурса госорганизации и исключая таким образом какой-либо технический ущерб.

Периметр исследования

В рамки исследования вошли наиболее крупные посещаемые государственные веб-ресурсы. Указанные веб-ресурсы были оценены по девяти критериям, которые позволили дать объективное заключение по уровню защищенности.

Периметр исследования

Полный перечень государственных веб-ресурсов официальные страницы которых вошли в периметр аудита указаны далее:

- Администрация Президента РК
- Управление Делами Президента РК
- Служба Государственной охраны РК
- Ассамблея народа Казахстана
- Национальная комиссия по делам женщин и семейно-демографической Политике
- Совет Безопасности РК
- Парламент
- Сенат
- Мажилис
- Верховный Суд РК
- Суд г. Астаны
- Алматинский городской суд
- Суд г. Шымкент
- Акмолинский областной суд
- Актюбинский областной суд
- Алматинский областной суд
- Атырауский областной суд
- Восточно-Казахстанский областной суд
- Жамбылский областной суд
- Западно-Казахстанский областной суд
- Карагандинский областной суд
- Костанайский областной суд
- Кызылординский областной суд
- Мангистауский областной суд

Периметр исследования

Полный перечень государственных веб-ресурсов официальные страницы которых вошли в периметр аудита указаны далее:

- Павлодарский областной суд
- Северо-Казахстанский областной суд
- Туркестанский областной суд
- Военный суд
- Генеральная прокуратура РК
- Конституционный Совет РК
- Комитет национальной безопасности РК
- Официальный информационный ресурс Премьер-Министра РК
- Электронное правительство
- Агентство РК по делам государственной службы
- Агентство по защите и развитию конкуренции РК
- Агентство РК по противодействию коррупции
- Агентство РК по регулированию и развитию финансового рынка
- Национальный Банк РК
- Министерство внутренних дел РК
- Министерство здравоохранения РК
- Министерство индустрии и инфраструктурного развития РК
- Министерство иностранных дел РК
- Министерство информации и общественного развития РК
- Министерство культуры и спорта РК
- Министерство национальной экономики РК
- Министерство обороны РК
- Министерство образования и науки РК
- Министерство по чрезвычайным ситуациям РК

Периметр исследования

Полный перечень государственных веб-ресурсов официальные страницы которых вошли в периметр аудита указаны далее:

- Министерство сельского хозяйства РК
- Министерство торговли и интеграции РК
- Министерство труда и социальной защиты населения РК
- Министерство финансов РК
- Министерство цифрового развития, инноваций и аэрокосмической промышленности РК
- Министерство экологии, геологии и природных ресурсов РК
- Министерство энергетики РК
- Министерство юстиции РК
- Счетный комитет по контролю за исполнением республиканского бюджета
- Центральная избирательная комиссия РК
- Антитеррористический центр РК
- Пограничная служба Комитета национальной безопасности РК
- Агентство по стратегическому планированию и реформам РК
- Уполномоченный по правам человека в РК
- Акимат г. Алматы
- Акимат г. Нур-Султан
- Акимат г. Шымкент
- Акимат Акмолинской области (г. Кокшетау)
- Акимат Актюбинской области (г. Актобе)
- Акимат Алматинской области (г. Талдыкорган)
- Акимат Атырауской области (г. Атырау)
- Акимат Восточно-Казахстанской области (г. Усть-Каменогорск)
- Акимат Жамбылской области (г. Тараз)
- Акимат Западно-Казахстанской области (г. Уральск)

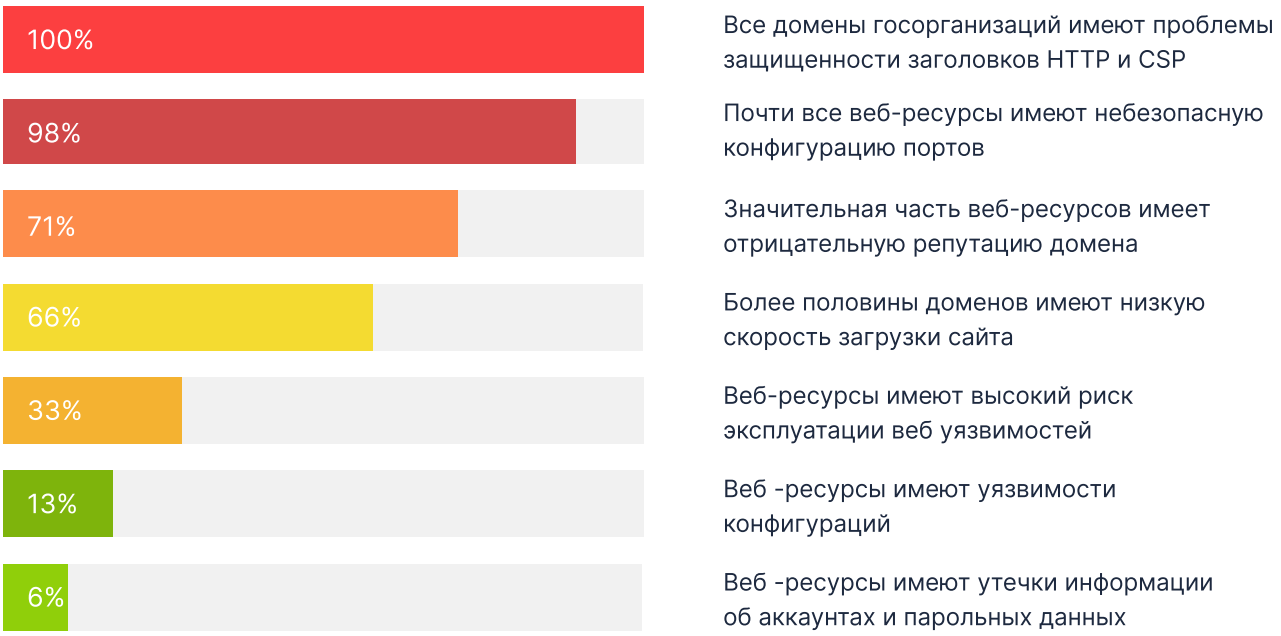
Периметр исследования

Полный перечень государственных веб-ресурсов официальные страницы которых вошли в периметр аудита указаны далее:

- Акимат Карагандинской области (г. Караганда)
- Акимат Кызылординской область (г. Кызылорда)
- Акимат Костанайской области (г. Костанай)
- Акимат Мангистауской области (г. Актау)
- Акимат Павлодарской области (г. Павлодар)
- Акимат Северо-Казахстанской области (г. Петропавловск)
- Акимат Туркестанской области (г. Туркестан)
- Акимат г. Семей
- Акимат г. Кентау
- Акимат г. Экибастуз
- Акимат г. Рудный
- Акимат г. Аркалык
- Акимат г. Жанаозен
- Акимат г. Темиртау
- Акимат г. Жезказган
- Акимат г. Балхаш
- Акимат г. Сатпаев
- Акимат г. Шахтинск
- Акимат г. Каскелен

Краткие результаты

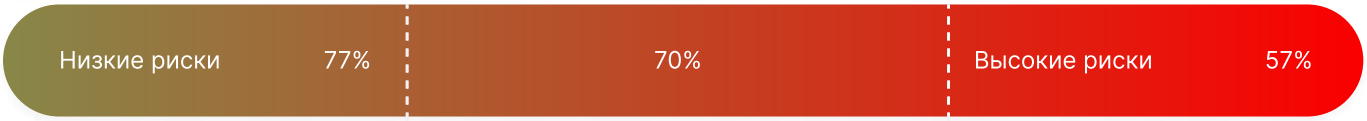
Далее описаны результаты анализа по выбранным критериям для 91 веб-ресурса.
Тестирование состояло из девяти ключевых точек контроля: производительность веб-сайта, репутация домена, состав программного обеспечения, HTTP заголовки безопасности, шифрование трафика, наличие утечек данных, сетевая безопасность, соответствие Security.txt, безопасность электронной почты.



Выводы по результатам анализа: на данный момент значительная часть официальных веб-страниц государственных организаций РК имеет уязвимости, которые могут быть использованы киберпреступниками с целью нанести урон деятельности веб-ресурса.

Краткие результаты

Далее приведены результаты оценки уровня защищенности веб-ресурсов госорганизаций РК. Средний показатель защищенности государственных веб-ресурсов составил 70%.



Ассамблея народа Казахстана
Национальная комиссия по делам женщин и семейно-демографической Политике
Костанайский областной суд
Совет Безопасности РК
Акимат Алматинской области
Верховный Суд РК
Суд г. Астаны
Алматинский городской суд
Суд г. Шымкент
Акмолинский областной суд
Алматинский областной суд
Атырауский областной суд
Атырауский областной суд
Восточно-Казахстанский областной суд
Жамбылский областной суд
Западно-Казахстанский областной суд
Карагандинский областной суд
Кызылординский областной суд
Мангистауский областной суд
Павлодарский областной суд
Северо-Казахстанский областной суд
Туркестанский областной суд
Военный суд
Комитет национальной безопасности РК
Электронное правительство
Генеральная прокуратура РК
Агентство РК по делам государственной службы

Агентство РК по противодействию коррупции
Агентство РК по регулированию и развитию финансового рынка Национальный Банк
Министерство внутренних дел
Министерство здравоохранения
Министерство индустрии и инфраструктурного развития
Министерство иностранных дел
Министерство информации и общественного развития
Министерство культуры и спорта
Министерство национальной экономики
Министерство обороны
Министерство образования и науки
Министерство по чрезвычайным ситуациям
Министерство сельского хозяйства
Министерство торговли и интеграции
Министерство труда и социальной защиты населения
Министерство финансов
Министерство цифрового развития, инноваций и аэрокосмической промышленности
Министерство экологии, геологии и природных ресурсов
Министерство энергетики
Министерство юстиции
Уполномоченный по правам человека
Агентство по стратегическому планированию и реформам
Пограничная служба Комитета национальной безопасности
Все областные акиматы
Центральная избирательная комиссия
Акимат г.Жанаозен
Акимат г.Экибастуз
Акимат г.Рудный
Акимат г.Аркалык
Акимат г.Жанаозен
Акимат г.Жезказган
Акимат г.Сатпаев
Акимат г.Семей
Акимат г.Кентау
Акимат г.Балхаш

Мажилис
Парламент
Сенат
Акимат г. Нур-Султан
Официальный информационный ресурс Премьер-Министра
Служба Государственной охраны
Управление Делами Президента
Администрация Президента
Счетный комитет по контролю за исполнением республиканского бюджета
Конституционный Совет
Акимат Актюбинской области

Краткие результаты

Далее приведены результаты оценки уровня защищенности веб-ресурсов. Согласно результатам оценки, которая состояла из девяти критериев таких как: репутация домена, шифрование трафика, утечка информации, открытые порты, Security. txt, безопасность email, состав программного обеспечения, скорость работы, HTTPS заголовки и безопасность контента – средний показатель защищенности составил 70%

Низкие риски

Веб-ресурсы, которые имеют показатель защищенности в диапазоне от 77% до 71%

Ассамблея народа Казахстана
Национальная комиссия по делам женщин и семейно-демографической Политике
Костанайский областной суд
Совет Безопасности РК
Акимат Алматинской области
Верховный Суд РК
Суд г. Астаны
Алматинский городской суд
Суд г. Шымкент
Акмолинский областной суд
Алматинский областной суд
Электронное правительство
Атырауский областной суд
Атырауский областной суд
Восточно-Казахстанский областной суд
Жамбылский областной суд
Западно-Казахстанский областной суд
Карагандинский областной суд
Кызылординский областной суд
Мангистауский областной суд
Павлодарский областной суд
Северо-Казахстанский областной суд
Туркестанский областной суд
Военный суд
Комитет национальной безопасности РК

Показатели рисков потенциальной эксплуатации веб-ресурса

Веб-ресурсы, которые имеют показатель защищенности 70%

Генеральная прокуратура
Агентство по делам государственной службы
Агентство по защите и развитию конкуренции
Агентство по противодействию коррупции
Агентство по регулированию и развитию финансового рынка
Национальный Банк
Министерство внутренних дел
Министерство здравоохранения
Министерство индустрии и инфраструктурного развития
Министерство иностранных дел
Министерство информации и общественного развития
Акимат г.Жанаозен
Акимат г.Жезказган
Акимат г.Сатпаев
Акимат г.Семей
Акимат г.Кентау
Акимат г.Балхаш
Министерство образования и науки
Министерство по чрезвычайным ситуациям
Министерство сельского хозяйства
Министерство торговли и интеграции РК
Министерство труда и социальной защиты населения РК
Министерство финансов РК
Министерство цифрового развития, инноваций и аэрокосмической промышленности РК
Министерство экологии, геологии и природных ресурсов РК
Министерство энергетики РК
Министерство юстиции РК
Уполномоченный по правам человека в Республике Казахстан
Агентство по стратегическому планированию и реформам РК
Министерство культуры и спорта РК
Министерство национальной экономики РК
Министерство обороны РК
Пограничная служба Комитета национальной безопасности РК
Все областные акиматы
Центральная избирательная комиссия РК
Акимат г. Жанаозен
Акимат г. Экибастуз
Акимат г. Рудный
Акимат г. Аркалык

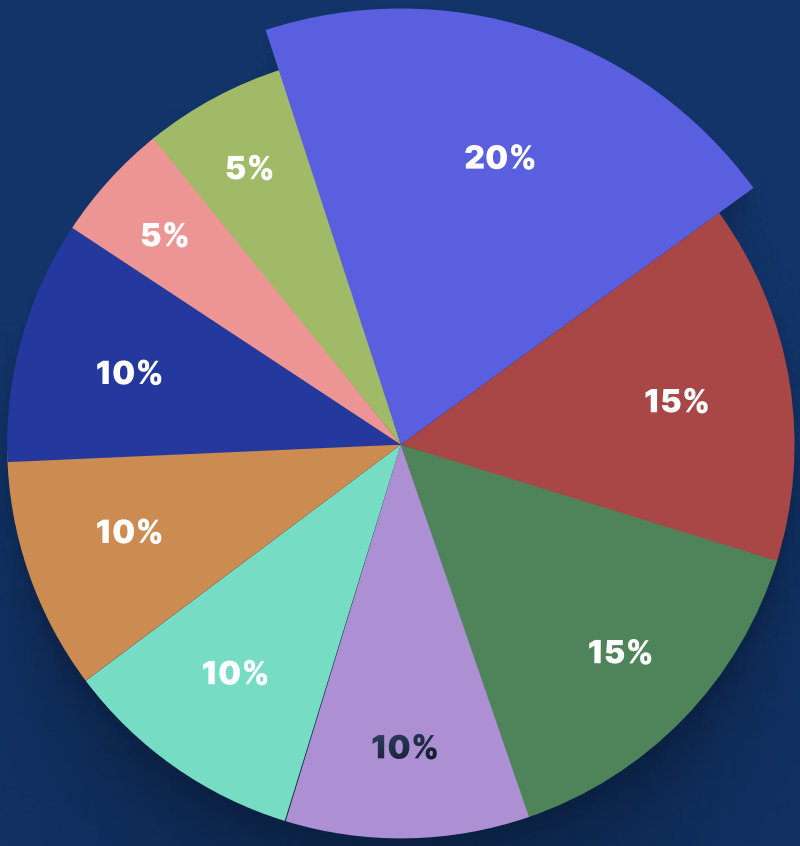
Высокие риски

Веб-ресурсы, которые имеют показатель защищенности менее 70%

Мажилис
Парламент
Сенат
Акимат г. Нур-Султан
Официальный информационный ресурс Премьер-Министра РК
Служба Государственной охраны РК
Управление Делами Президента РК
Администрация Президента РК
Счетный комитет по контролю за исполнением республиканского бюджета
Конституционный Совет РК
Акимат Актюбинской области

Методология расчетов

Уровень защищенности официальных государственных веб-страниц оценивался по девяти критериям имеющим различное влияние на финальную оценку. Степень влияния определялась исходя из рисков, которые влекут за собой уязвимости разного типа. Детализация по степени влияния на финальную оценку защищенности представлена далее:



Утечка данных	20%	Состав программного обеспечения	10%
Шифрование данных	15%	Security.txt	10%
Безопасность почтового сервиса	15%	Скорость работы	5%
Репутация домена	10%	HTTPS заголовки безопасности контента	5%
Открытые порты	10%		

Основные результаты

Шифрование трафика

Описание критерия: согласно мировым стандартам, личные данные, которые передаются между веб-сервисом и клиентом, подлежат шифрованию. Практика шифрования данных при передаче обеспечивает надежную защиту от перехвата логинов и паролей людьми, которые находятся в одной сети.

Описание потенциальной атаки: в ситуациях когда трафик не зашифрован на должном уровне, передаваемые сообщения могут быть перехвачены или изменены по средствам атаки типа «человек посередине».

Негативные последствия: злоумышленникам могут быть доступны все отправляемые пользователем данные (логин, пароль, ПИН-код и т. п.). Приводит к утечке данных клиентов, финансовым убыткам.

Детальный анализ и перечень проверок, которые проводились относительно шифрования трафика приведен далее:

- Рейтинг (SSL Lab)
- Недостатки в конфигурировании алгоритма Диффи – Хеллмана
- Уязвимость POODLE
- Уязвимость FREAK
- Возможность проведения атаки Logjam
- Уязвимость ROBOT
- Уязвимость Beast
- Поддержка NPN и ALPN
- Уязвимость CVE-2016-2107
- Уязвимость Heartbleed
- Уязвимость Ticketbleed
- SSL Renegotiation
- Поддержка RC4
- Поддержка Forward Secrecy
- Версия TLS
- Поддержка SSL 2.0 и SSL 3.0

Отсутствуют уязвимости

Обнаружены уязвимости

Основные результаты

Шифрование трафика

Уязвимости связанные с шифрованием передаваемых данных были обнаружены на следующих веб-страницах:

Администрация Президента РК

Управление Делами Президента РК

Служба Государственной охраны РК

Парламент

Сенат

Мажилис

Конституционный Совет РК

Комитет национальной безопасности РК

Счетный комитет по контролю за исполнением республиканского бюджета

Центральная избирательная комиссия РК

Акимат г. Нур-Султан

Акимат Актюбинской области (г. Актобе)

Основные результаты

Состав программного обеспечения

В данном разделе описаны результаты, которые могут охарактеризовать риск эксплуатации веб-уязвимостей, таких как SQL Injection, Cross Site Scripting, Broken Authentication and Session Management, Insecure Direct Object References, Cross Site Request Forgery, Security Misconfiguration, Insecure Cryptographic Storage, Failure to restrict URL Access, Insufficient Transport Layer Protection, Unvalidated Redirects and Forwards. Подробнее можно ознакомиться по ссылке https://www.owasp.org/ .
Была проведена проверка первой главной страницы госорганизации.

Уязвимость: использование устаревшей версии программного обеспечения, которая не поддерживается разработчиком. Не обновлена CMS или ее компоненты.
Риск: с высокой вероятностью существует эксплоит, который позволит злоумышленникам проэксплуатировать уязвимости старых версий.

Негативные последствия: неправомерный доступ к данным.

Детальный анализ приведен далее:

Основные результаты

Состав программного обеспечения

Следующие веб-ресурсы имеют высокий риск атак OWASP Топ 10:

Администрация Президента РК

Управление Делами Президента РК

Служба Государственной охраны Республики Казахстан

Ассамблея народа Казахстана

Национальная комиссия по делам женщин и семейно-демографической о Политике

Совет Безопасности РК

Сенат

Верховный Суд РК

Суд г. Астаны

Алматинский городской суд

Суд г. Шымкент

Акмолинский областной суд

Актюбинский областной суд

Алматинский областной суд

Атырауский областной суд

Восточно-Казахстанский областной суд

Жамбылский областной суд

Западно-Казахстанский областной суд

Карагандинский областной суд

Кызылординский областной суд

Мангистауский областной суд

Павлодарский областной суд

Северо-Казахстанский областной суд

Туркестанский областной суд

Военный суд

Конституционный Совет РК

Комитет национальной безопасности РК

Официальный информационный ресурс Премьер-Министра Республики Казахстан

Электронное правительство

Акимат Актюбинской области

Основные результаты

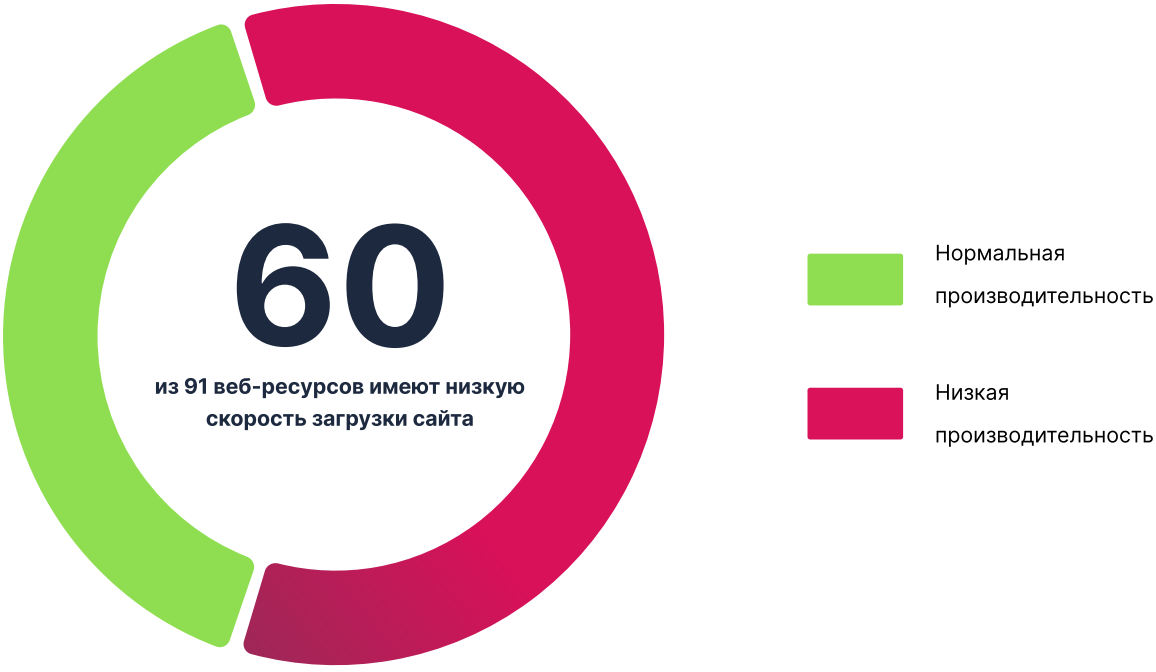
Скорость загрузки

Описание критерия: оценка скорости загрузки основана на данных FCP и FID, полученных методом имитации загрузки сайта. Тестирование наилучшей практики производительности выполняется для анализа устойчивости сайта к нагрузкам.

Описание потенциальной атаки: низкая производительность позволит злоумышленникам перегружать веб-ресурс путем специально подобранных запросов, тем самым затруднив или полностью прекратив доступ граждан к веб-ресурсу.

Негативные последствия: недоступность веб-ресурса для пользователей.

Детальный анализ приведен далее:



Основные результаты

Скорость загрузки

Следующие веб-ресурсы имеют низкую производительность:

Служба Государственной охраны Республики Казахстан
Национальная комиссия по делам женщин и семейно-демографической Политике
Конституционный Совет РК
Акимат г. Алматы
Акимат Жамбылской области (г. Тараз)
Министерство финансов Республики Казахстан
Министерство труда и социальной защиты населения Республики Казахстан
Акимат Акмолинской области (г. Кокшетау)
Агентство РК по делам государственной службы
Министерство по чрезвычайным ситуациям Республики Казахстан
Акимат Костанайской области (г. Костанай)
Акимат Туркестанской области (г. Туркестан)
Министерство образования и науки Республики Казахстан
Министерство экологии, геологии и природных ресурсов Республики Казахстан
Акимат Западно-Казахстанской области (г. Уральск)
Акимат Карагандинской области (г. Караганда)
Уполномоченный по правам человека в Республике Казахстан
Агентство по защите и развитию конкуренции РК
Акимат Мангистауской области (г. Актау)
Пограничная служба Комитета национальной безопасности Республики Казахстан
Агентство РК по регулированию и развитию финансового рынка
Министерство индустрии и инфраструктурного развития Республики Казахстан
Министерство энергетики Республики Казахстан
Акимат Кызылординской область (г. Кызылорда)
Акимат Северо-Казахстанской области (г. Петропавловск)
Ассамблея народа Казахстана
Министерство здравоохранения РК
Антитеррористический центр РК
Акимат г. Семей
Акимат г. Экибастуз
Акимат г. Каскелен
Министерство торговли и интеграции Республики Казахстан
Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан
Акимат Восточно-Казахстанской области (г. Усть-Каменогорск)
Акимат Павлодарской области (г. Павлодар)
Агентство по стратегическому планированию и реформам Республики Казахстан
Агентство РК по противодействию коррупции
Министерство национальной экономики Республики Казахстан
Счетный комитет по контролю за исполнением республиканского бюджета
Акимат г. Шымкент
Акимат г. Сатпаев
Министерство иностранных дел Республики Казахстан
Министерство культуры и спорта Республики Казахстан
Акимат Атырауской области (г. Атырау)
Акимат г. Рудный
Министерство юстиции Республики Казахстан
Генеральная прокуратура РК
Министерство внутренних дел РК
Министерство обороны Республики Казахстан
Акимат г. Жанаозен
Акмолинский областной суд
Министерство информации и общественного развития Республики Казахстан
Министерство сельского хозяйства РК
Акимат г. Кентау
Акимат г. Шахтинск
Акимат г. Аркалык
Акимат г. Темиртау
Акимат г. Жезказган
Акимат г. Балхаш
Электронное правительство

Основные результаты

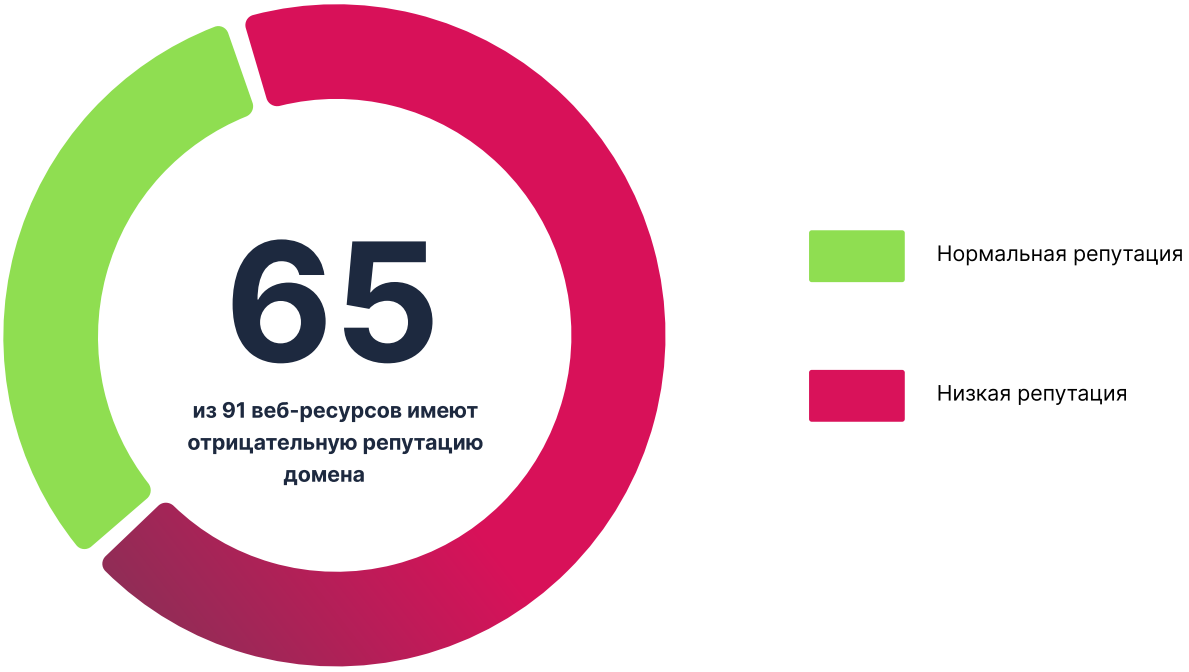
Репутация домена

Описание критерия: анализ открытых источников содержащих рейтинги доменов в сети интернет.

Описание потенциальной атаки: если веб-ресурс занесен в черный список, доступ на него может быть заблокирован браузерами или иными системами.

Негативные последствия: это в первую очередь приводит к потере трафика, доверия клиентов и, следовательно, денег. Проверка репутации домена в различных базах антивирусных ПО.

Детальный анализ приведен далее:



Основные результаты

Репутация домена

Следующие веб-ресурсы имеют отрицательную репутацию домена:

Парламент
Сенат
Мажилис
Совет Безопасности РК
Официальный информационный ресурс Премьер-Министра РК
Администрация Президента РК
Генеральная прокуратура РК
Конституционный Совет РК
Комитет национальной безопасности РК
Электронное правительство
Агентство РК по делам государственной службы
Агентство по защите и развитию конкуренции РК
Агентство РК по противодействию коррупции
Агентство РК по регулированию и развитию финансового рынка
Национальный Банк РК
Министерство внутренних дел РК
Министерство здравоохранения РК
Министерство индустрии и инфраструктурного развития РК
Министерство иностранных дел Республики Казахстан
Министерство информации и общественного развития РК
Министерство культуры и спорта РК
Министерство национальной экономики РК
Министерство обороны РК
Министерство образования и науки РК
Министерство по чрезвычайным ситуациям РК
Министерство сельского хозяйства РК
Министерство торговли и интеграции РК
Министерство труда и социальной защиты населения РК
Министерство финансов РК
Акимат г. Балхаш
Акимат г. Сатпаев
Акимат г. Шахтинск
Министерство цифрового развития, инноваций и аэрокосмической промышленности РК
Министерство экологии, геологии и природных ресурсов РК
Министерство энергетики РК
Министерство юстиции РК
Счетный комитет по контролю за исполнением республиканского бюджета
Акимат г. Алматы
Акимат г. Шымкент
Акимат Акмолинской области
Акимат Актюбинской области
Акимат Атырауской области
Акимат Восточно-Казахстанской области
Акимат Жамбылской области
Акимат Западно-Казахстанской области
Акимат Карагандинской области
Акимат Кызылординской область
Акимат Костанайской области
Акимат Мангистауской области
Акимат Павлодарской области
Акимат Северо-Казахстанской области
Акимат Туркестанской области
Антитеррористический центр РК
Пограничная служба Комитета национальной безопасности РК
Агентство по стратегическому планированию
Акимат г. Семей
Акимат г. Кентау
Акимат г. Экибастуз
Акимат г. Рудный
Акимат г. Аркалык
Акимат г. Жанаозен
Акимат г. Темиртау
Акимат г. Жезказган
Акимат г. Каскелен

Основные результаты

HTTP заголовки безопасности

Описание критерия: при передаче данных от веб-сервера к клиенту, могут передаваться мета–данные, которые могут быть использованы при атаке. В процессе аудита проверялись такие заголовки как: Strict-Transport-Security, Content-Security-Policy, X-XSS-Protection, HTTP Strict-Transport-Security, X-Frame-Options, Expect-CT.

Описание потенциальной атаки: атаки направленные на добавления вредоносного содержания в структуру веб-ресурса, такие, как инъекция вредоносного кода, XSS и изменения контента веб-ресурса.

Негативные последствия: несанкционированный доступ к данным, получение злоумышленником контроля над веб-ресурсом.

Детальный анализ приведен далее:

Основные результаты

Утечки информации об аккаунтах и парольных данных

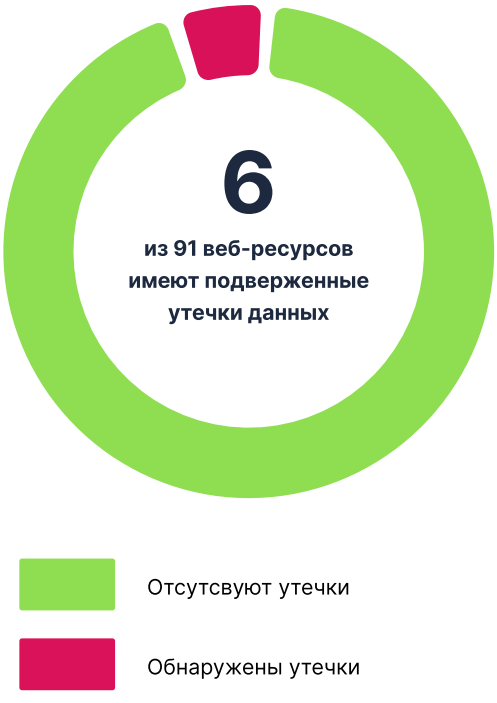
Описание критерия: любая утечка информации несет в себе негативные финансовые, репутационные последствия для компании.

В результате взлома различных сервисов в сети появляются сотни данных утекших почтовыхадресов, паролей и другой персональной информации. Данные базы попадают в сеть огромными объемами. Известные случаи связаны с такими компаниями как «Сбербанк», «Билайн», «OZON», когда 450 тысяч паролей и email пользователей были обнаружили на одном из сайтов с утечками.
Уязвимость: использование сотрудниками корпоративной почты организации при регистрации на различных сервисах. Так зачастую, в 90% случаев пароли учетныхзаписей пользователей на различных сервисах совпадают.

Описание потенциальной атаки: получение доступа к внутренней почте, рабочей переписке, рабочей документации компании, полученный доступ к чувствительной информации злоумышленниками может быть использован для осуществления атаки на информационные системы государственных организаций.

Негативные последствия: неправомерный доступ к данным, финансовые и репутационные потери.

Детальный анализ приведен далее:



Следующие веб-ресурсы имеют утечки данных:

Электронное правительство
Национальный Банк РК
Акимат г. Нур-Султан
Парламент
Сенат
Мажилис

Основные результаты

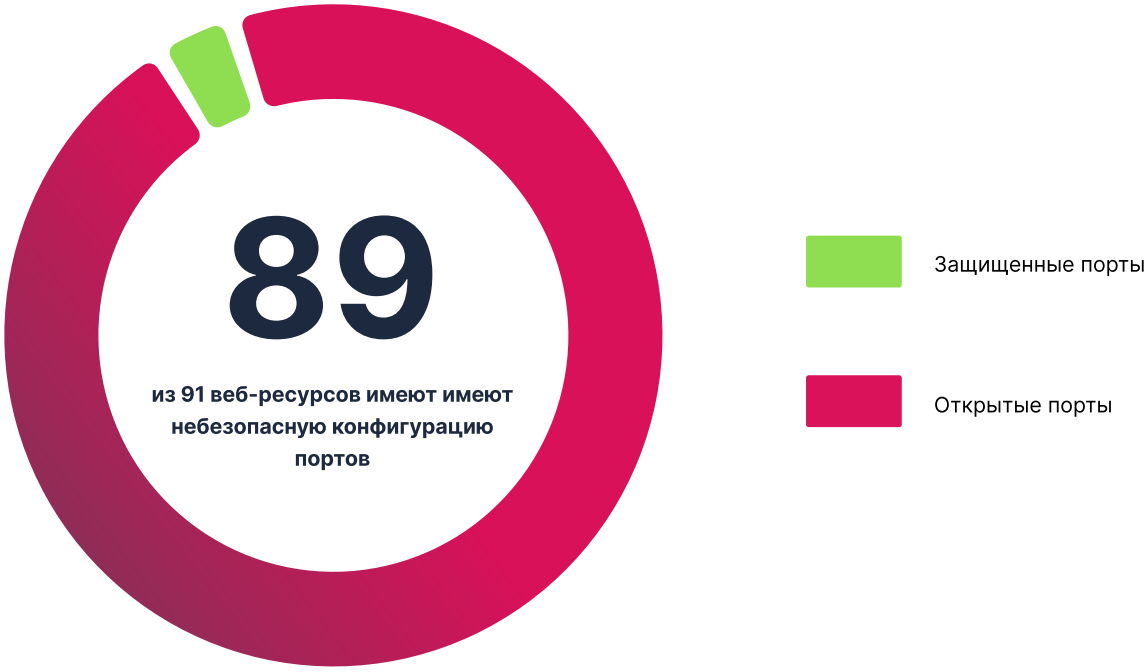
Безопасность сети

Описание критерия: был проведен анализ портов, которые не используются напрямую самим веб-сервером. Анализ был направлен на выявления потенциально опасных портов, которые могут быть использованы злоумышленниками.

Описание потенциальной атаки: неправомерный доступ и получение контроля над внутренними информационными ресурсами злоумышленниками.

Негативные последствия: неправомерный доступ к данным, финансовые и репутационные потери.

Детальный анализ приведен далее:



Основные результаты

Безопасность сети

Следующие веб-ресурсы имеют проблемы с безопасностью сети:

Агентство по стратегическому планированию и реформам Республики Казахстан
Акимат Северо-Казахстанской области
Акимат Карагандинской области
Пограничная служба Комитета национальной безопасности РК
Министерство экологии, геологии и природных ресурсов РК
Агентство по защите и развитию конкуренции РК
Министерство индустрии и инфраструктурного развития РК
Акимат Алматинской области
Администрация Президента РК
Управление Делами Президента РК
Служба Государственной охраны РК
Акимат г. Сатпаев
Министерство обороны РК
Министерство образования и науки РК
Министерство сельского хозяйства РК
Министерство торговли и интеграции РК
Военный суд
Мангистауский областной суд
Павлодарский областной суд
Северо-Казахстанский областной суд
Туркестанский областной суд
Военный суд
Национальный Банк РК
Министерство внутренних дел РК
Министерство здравоохранения РК
Акимат Жамбылской области
Министерство культуры и спорта РК
Акимат г. Рудный
Акимат г. Темиртау
Министерство цифрового развития, инноваций и аэрокосмической промышленности РК
Акимат Туркестанской области
Акимат Западно-Казахстанской области
Счетный комитет по контролю за исполнением республиканского бюджета
Официальный информационный ресурс Премьер-Министра РК
Агентство РК по противодействию коррупции
Министерство информации и общественного развития РК
Акимат Павлодарской области
Совет Безопасности РК
Парламент
Сенат
Мажилис
Верховный Суд РК
Суд г. Астаны
Алматинский городской суд
Суд г. Шымкент
Акмолинский областной суд
Актюбинский областной суд
Алматинский областной суд
Атырауский областной суд
Восточно-Казахстанский областной суд
Жамбылский областной суд
Западно-Казахстанский областной суд
Карагандинский областной суд
Костанайский областной суд
Кызылординский областной суд
Министерство иностранных дел РК
Акимат г. Аркалык
Акимат г. Жезказган
Акимат Атырауской области
Акимат г. Каскелен
Акимат г. Шахтинск
Акимат Кызылординской область
Акимат Восточно-Казахстанской области
Министерство труда и социальной защиты населения РК
Агентство РК по делам государственной службы
Агентство РК по регулированию и развитию финансового рынка
Уполномоченный по правам человека в Республике Казахстан
Министерство национальной экономики
Акимат г. Алматы
Акимат г. Нур-Султан
Акимат г. Шымкент
Акимат Акмолинской области
Акимат Актюбинской области
Министерство финансов РК
Министерство по чрезвычайным ситуациям
Министерство энергетики РК
Министерство юстиции РК
Генеральная прокуратура РК
Конституционный Совет РК
Комитет национальной безопасности РК
Электронное правительство
Центральная избирательная комиссия РК
Антитеррористический центр РК
Акимат Костанайской области
Акимат Мангистауской области
Акимат г. Кентау
Акимат г. Экибастуз
Акимат г. Жанаозен
Акимат г. Балхаш

Основные результаты

Security.txt

Когда независимые исследователи безопасности обнаруживают угрозу в веб-сервисах, у них часто не хватает каналов связи с владельцем веб-сервиса для сообщения о раскрытии уязвимости. В результате о проблемах безопасности не сообщается. Security.txt определяет стандарт, чтобы помочь организациям определить, как исследователи в области безопасности могут безопасно раскрывать уязвимости.

Уязвимость: выявленные уязвимости могут остаться не известными для владельцев веб -ресурса.
Риск: уязвимость может быть эксплуатирована злоумышленниками.

Негативные последствия: несанкционированный доступ к информации, в обход существующих правил разграничения доступа; снижение производительности, аварийные завершения и недоступность сервисов.

В результате 100% госорганизаций не прошли проверку Security.txt compliance.

Детальный анализ приведен далее:

Основные результаты

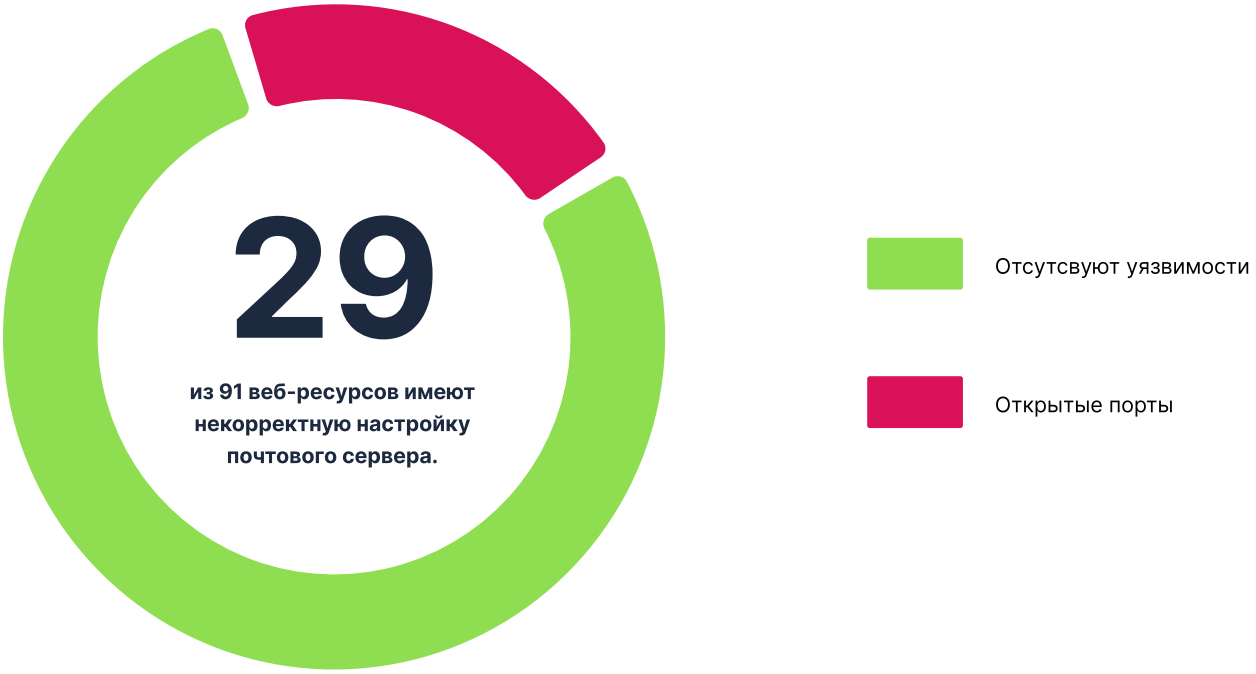
Email security

Описание критерия: более 90% почтового трафика содержит спам, фишинг, вредоносные программы и другие электронные угрозы. Электронная почта является основным вектором заражения для вымогателей и вредоносных программ. Данный пункт проверяет, правильно ли настроен почтовый сервер веб-ресурса для предотвращения этих распространенных угроз.

Описание потенциальной атаки: почта является наиболее вероятным способом заражения вредоносными программными продуктами.

Негативные последствия: получение нежелательной почтовой рассылки, несущей бесполезную информацию и содержащей в себе вредоносный код (бот-сети, трояны, черви), вектор для проведения фишинга.

Детальный анализ приведен далее:



Основные результаты

Email security

Следующие веб-ресурсы имеют проблемы с почтовым сервером:

Администрация Президента РК

Управление Делами Президента РК

Служба Государственной охраны РК

Национальная комиссия по делам женщин и семейно-демографической Политике

Парламент

Сенат

Мажилис

Верховный Суд РК

Суд г. Астаны

Алматинский городской суд

Суд г. Шымкент

Акмолинский областной суд

Актюбинский областной суд

Алматинский областной суд

Атырауский областной суд

Восточно-Казахстанский областной суд

Жамбылский областной суд

Западно-Казахстанский областной суд

Карагандинский областной суд

Костанайский областной суд

Кызылординский областной суд

Мангистауский областной суд

Павлодарский областной суд

Северо-Казахстанский областной суд

Туркестанский областной суд

Военный суд

Комитет национальной безопасности РК

Национальный Банк РК

Акимат Алматинской области (г. Талдыкорган)

Основной вывод

В ходе исследования безопасности веб-ресурсов госорганизаций РК, эксперты ЦАРКА проверили соблюдение общедоступных рекомендаций по настройке веб-серверов и взаимосвязанных компонентов.

Согласно выбранным критериям и методике, средний показатель защищенности государственных веб-ресурсов составил 70%.

Результат исследования показал, что на веб-ресурсах госорганизаций РК присутствуют достаточно известные уязвимости и проблемы безопасности. Текущий уровень защиты значимых госорганизаций дает возможность потенциальным злоумышленникам реализовать атаки на эти веб-ресурсы.

Заключение

Проведенное исследование продуктом WebTotem указало на ряд слабых и уязвимых мест госорганизаций РК, которые при кажущейся только на первый взгляд мало значимости и трудности в реализации злоумышленниками, могут в дальнейшем привести к крупным финансовым, репутационным потерям.

В целях обеспечения целостности информационных систем государства и защиты персональных данных граждан, государственным органам необходимо найти и устранить уязвимости в своих системах.

В рамках реализации концепции кибербезопасности "Киберщит Казахстана", утвержденной постановлением Правительства Республики Казахстан от 30 июня 2017 года № 407, продукт WebTotem помогает в достижении и поддержании уровня защищенности электронных информационных ресурсов и информационных систем государственных органов РК от внешних и внутренних угроз.

В настоящее время ОЮЛ «ЦАРКА» готова предоставить на бесплатной основе годовое использование инструмента WebTotem для государственных органов РК для налаживания системы управления информационной безопасности и обеспечения надежной защиты.

О компании

WEBTOTEM

a monitoring system designed to protect web resources from intrusions and cyber threats

Применение лучших мировых практик по обеспечению информационной безопасности.

Выбор Global innovation through science and technology при поддержке правительства США

The best SaaS & B2B solution at the Echelon Asia Summit in Singapore in 2018

Top 3 on Latitude

Выбор TechCrunch Top Picks for Disrupt 2020

Top 3 on Emerge

Мы сканируем и мониторим более 150 000 Казахстанских сайтов в доменной зоне .kz

КЛИЕНТ WEBTOTEM МОЖЕТ

Миссия WebTotem заключается в том, чтобы донести революционный продукт, построенный на основе искусственного интеллекта, до людей из нетехнической сферы, чтобы они имели возможность защитить свой бизнес в один клик.

Предотвращать взломы с помощью пошаговых рекомендаций по обеспечению безопасности

Получать проактивную защиту от новых киберугроз

Оценивать и управлять рисками кибербезопасности

Мы поднимаем уровень информационной безопасности бизнес-сайтов по всему миру.

О компании

ОЮЛ «Центр анализа и расследования кибер атак» (далее - ЦАРКА) - одна из ведущих организаций в области информационной безопасности в Центральной Азии. Организация была образована в 2015 году, и за время своего существования завоевала признание специалистов по информационной безопасности по всему миру. Первый частный CERT в Казахстане.

Организация предоставляет широкий спектр услуг в области оценки защищенности, в том числе проведение аудитов ИБ и тестирований на проникновение, анализ защищенности информационных систем и бизнес-приложений, веб приложений, информационных инфраструктур.

Более 50 экспертов. Эксперты ЦАРКА обладают сертификатами OSCP, OSWP, CHFI, CISA, CCNA Security, ISO/IEC 27001—2015, OSCE и CEH и регулярно принимают участие в международных конференциях, таких как PHDays, ZeroNights, Инфофорум, КодИБ.

Эксперты организации являются авторами публикаций на таких ресурсах как журнал Хакер, HabraHabr, DigitalReport, ProfIT.kz и др.

Команда ЦАРКА занимала 1, 2 и 5 места в соревновании The Standoff на международной конференции по информационной безопасности PositiveHackDays с 2017 по 2020 года.

Контакты

г.Нур-Султан, проспект
Мангилик Ел 19/2 93кв

info@wtotem.com
wtotem.com