КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КАК УСТРАНИТЬ ТОП-10 УЯЗВИМОСТЕЙ СЕТЕВОЙ ЗАЩИТЫ

Дмитрий Хомутов

Директор по развитию
Компания «Айдеко»

+7-922-200-8230
d.homutov@ideco.ru
facebook.com/dhomutov

КОМПАНИЯ АЙДЕКО

Команда специалистов по безопасности, системных инженеров и разработчиков с многолетним опытом администрирования и системного программирования создают удобный и «умный» межсетевой экран нового поколения.

Мы используем собственные ноу-хау и базы данных, создаваемые с помощью технологий машинного обучения и искусственного интеллекта.

Более 14 000 компаний защищает Ideco UTM

Более 25 000 атак ежедневно блокируют наши решения

IDECO UTM ИСПОЛЬЗУЮТ

- Генеральная прокуратура Республики Казахстан
- ГУ «Управление Делами Президента Республики Казахстан»
- РГП «Дирекция административных зданий Администрации Президента и Правительства РК»
- АО «Национальная горнорудная компания «Тау-Кен Самрук»
- Кремниевый завод ТОО «Tau-Ken Temir»
- АО «АрселорМиттал Темиртау»
- АО «Мангистаумунайгаз»
- АО «Международный аэропорт Актау»
- ТОО «БАЙКЕН-U» (КАЗАТОМПРОМ)
- АО «РАХАТ»
- КАЗНИТУ ИМ. К.И.САТПАЕВА
- АО «Баян Сулу»

ИССЛЕДОВАНИЕ 2019 ГОДА

Мы проверили:

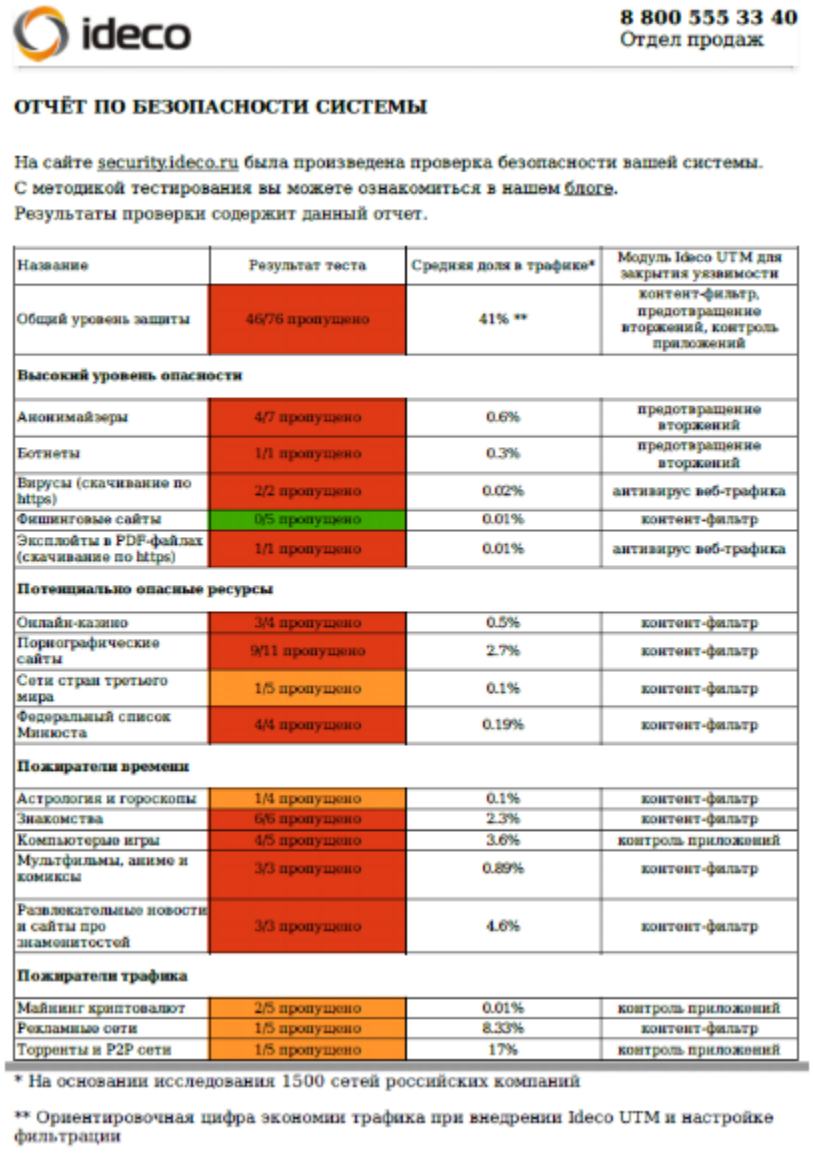
- 5000 локальных сетей в компаниях
  от 20 до 20 000 интернет-пользователей
- Информацию о 3000 попытках атак в сетях,
  которые защищает ideco utm

IDECO SECURITY

Online-Сервис проверяет:

- доступ к вредоносным и потенциально опасным сайтам;
- 15 категорий сайтов, более 120 URL;
- возможность прохождения вирусного трафика.

SECURITY.IDECO.RU



ideco

8 800 555 33 40
Отдел продаж

ОТЧЁТ ПО БЕЗОПАСНОСТИ СИСТЕМЫ

На сайте security.ideco.ru была произведена проверка безопасности вашей системы.
С методикой тестирования вы можете ознакомиться в нашем блоге.
Результаты проверки содержит данный отчет.

Название	Результат теста	Средняя доля в трафике*	Модуль Ideco UTM для закрытия уязвимости
Общий уровень защиты	46/76 пропущено	41% **	контент-фильтр, предотвращение вторжений, контроль приложений
Высокий уровень опасности			
Анонимайзеры	4/7 пропущено	0.6%	предотвращение вторжений
Ботнеты	1/1 пропущено	0.3%	предотвращение вторжений
Вирусы (скачивание по https)	2/2 пропущено	0.02%	антивирус веб-трафика
Фишинговые сайты	0/5 пропущено	0.01%	контент-фильтр
Эксплойты в PDF-файлах (скачивание по https)	1/1 пропущено	0.01%	антивирус веб-трафика
Потенциально опасные ресурсы			
Онлайн-казино	3/4 пропущено	0.5%	контент-фильтр
Порнографические сайты	9/11 пропущено	2.7%	контент-фильтр
Сети стран третьего мира	1/5 пропущено	0.1%	контент-фильтр
Федеральный список Минюста	4/4 пропущено	0.19%	контент-фильтр
Пожиратели времени			
Астрология и гороскопы	1/4 пропущено	0.1%	контент-фильтр
Знакомства	6/6 пропущено	2.3%	контент-фильтр
Компьютерные игры	4/5 пропущено	3.6%	контроль приложений
Мультфильмы, аниме и комиксы	3/3 пропущено	0.89%	контент-фильтр
Развлекательные новости и сайты про знаменитостей	3/3 пропущено	4.6%	контент-фильтр
Пожиратели трафика			
Майнинг криптовалют	2/5 пропущено	0.01%	контроль приложений
Рекламные сети	1/5 пропущено	8.33%	контент-фильтр
Торренты и P2P сети	1/5 пропущено	17%	контроль приложений

* На основании исследования 1500 сетей российских компаний

** Ориентировочная цифра экономии трафика при внедрении Ideco UTM и настройке фильтрации

IDECO SECURITY

Дополнительные проверки:

- почтовые адреса на компрометацию (по базе из более чем 7 млрд. адресов);
- информацию о скачанных торрентах;
- наличие ip-адреса в черных списках;
- открытые порты и ответы сервисов на внешнем интерфейсе.

SECURITY.IDECO.RU

Проверка почтового адреса на компрометацию:

Адрес	Найденные в базах пароли
[redacted]	не найдены

Информация о скачанных торрентах:

Дата (UTC)	Тип	Название	Размер
Jun 21, 2019, 7:48:49 PM	Игры	K3TDM.iso	1.58Гб
Jun 21, 2019, 5:52:48 PM	Игры	The Sims 2 Antology	8.35Гб
Jun 21, 2019, 5:37:06 PM	Игры	Sea Dogs To Each His Own [qoob RePack]	3.42Гб

Наличие IP-адреса в черных списках:

Название сервиса	Результат
Barracuda BBL	Clear
Sorbs.net	Clear
South Korean NBL	Low Risk
Spamcop	Listed
Spamhaus	Clear

Если вы используете статический IP-адрес, то его наличие в чёрных списках — серьёзный симптом участия хостов вашей сети в ботнетах. Рекомендации по устранению заражения.

Результаты сканирования вашего IP-адреса ([redacted])

Открытые порты:

80, 6881

Внимание! Веб-ресурсы рекомендуется публиковать защищая их модулем Web Application Firewall.

Порт	Сервис	Ответ сервиса
80, tcp	http	HTTP/1.1 200 OK Server: Virtual Web 0.9 Set-Cookie: SessionID=; path=/ Content-Type: text/html Content-Length: 151
		DHT Nodes 118.198.73.73 61937 187.233.235.179 42715 60.135.12.62 39204 94.82.177.149 24537 116.141.118.204 41312 199.161.234.168 11992 229.90.194.183 29788 239.134.37.73 48314 224.2.210.103 30581 29.143.11.176 30516 25.229.26.110

РЕЗУЛЬТАТ ТЕСТИРОВАНИЯ

98% межсетевых экранов не используют фильтрацию HTTPS-трафика

97% сетей не блокируют «пожиратели трафика»

ДОЛЯ “ПАРАЗИТНОГО ТРАФИКА”

Анонимайзеры	0,60%
Порнографические сайты	2,70%
Знакомства	2,30%
Компьютерные игры	3,60%
Мультфильмы, аниме и комиксы	0,89%
Развлекательные новости	4,60%
Рекламные сети	8,33%
Торренты и P2P сети	17%
	40,02%

* на основе исследования 1500 сетей российских компаний

ПРОБЛЕМА №1

Ограниченная ширина интернет-канала и безграничные потребности в трафике.

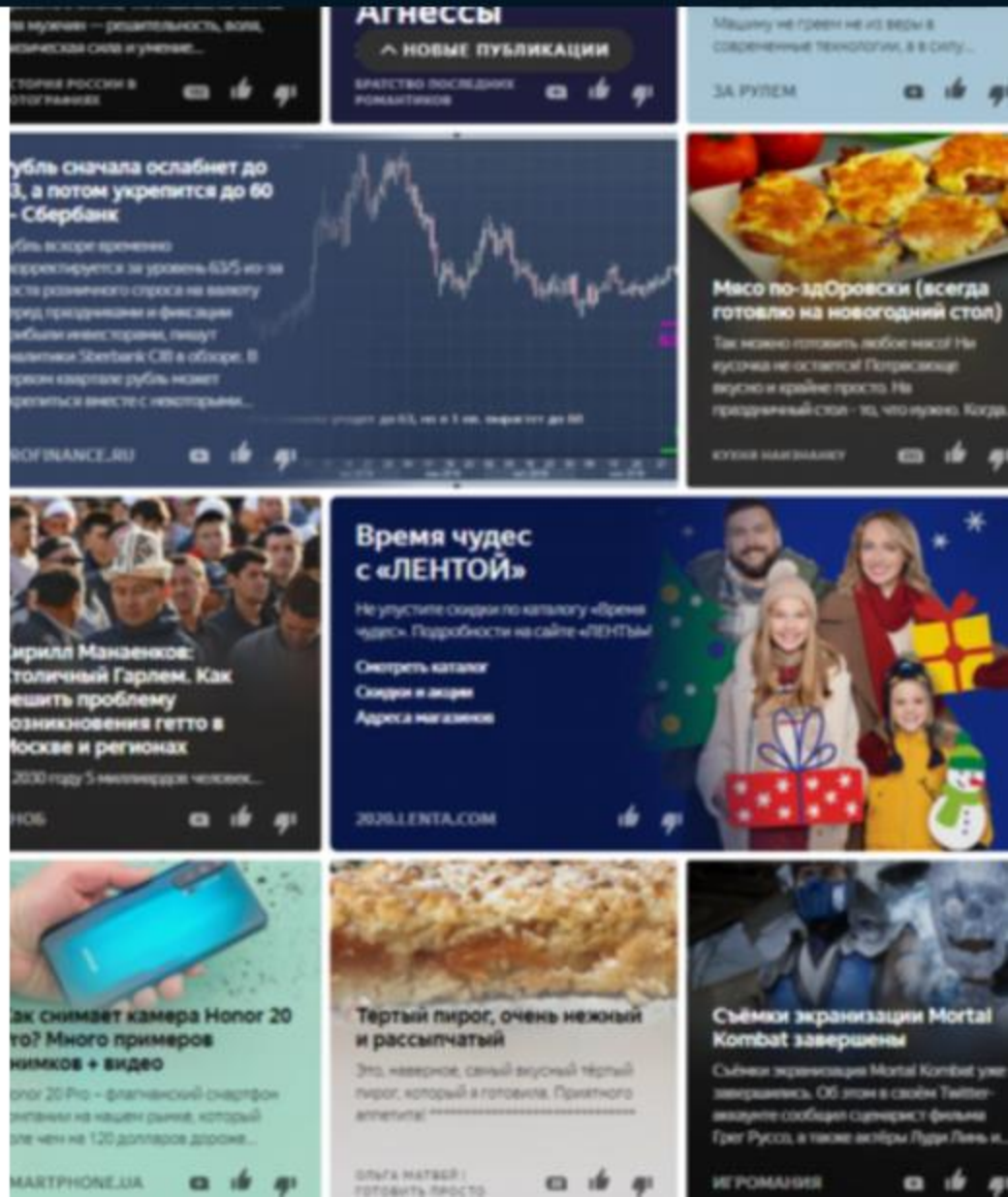
Медленный и нестабильный интернет для требуемых по работе ресурсов.

ПРОБЛЕМА №2

кража времени: развлекательные и фейковые новости, соц. сети, форумы.

Кража внимания: кликбейт, ремаркетинг, баннеры, всплывающие окна.

Кража мотивации: секс-контент, дофаминовая гиперстимуляция.



ПРОБЛЕМА №3

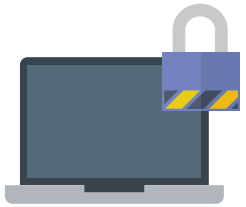
- отсутствие или нехватка компетентных специалистов по ит/иб;
- нет времени или опыта для работы с новыми решениями;
- нет бюджета на иб (кроме антивируса);
- работает - и ладно, не будем трогать, лишь бы не сломать.

СОДЕЙСТВИЕ РАЗВИТИЮ АТАК

Бесконтрольный выход в интернет

Информация в открытом виде

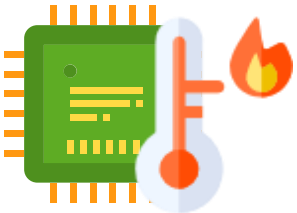
Бесконтрольный доступ между локальными сетями



Публикация корпоративных данных

Удалённый доступ

Анонимайзеры

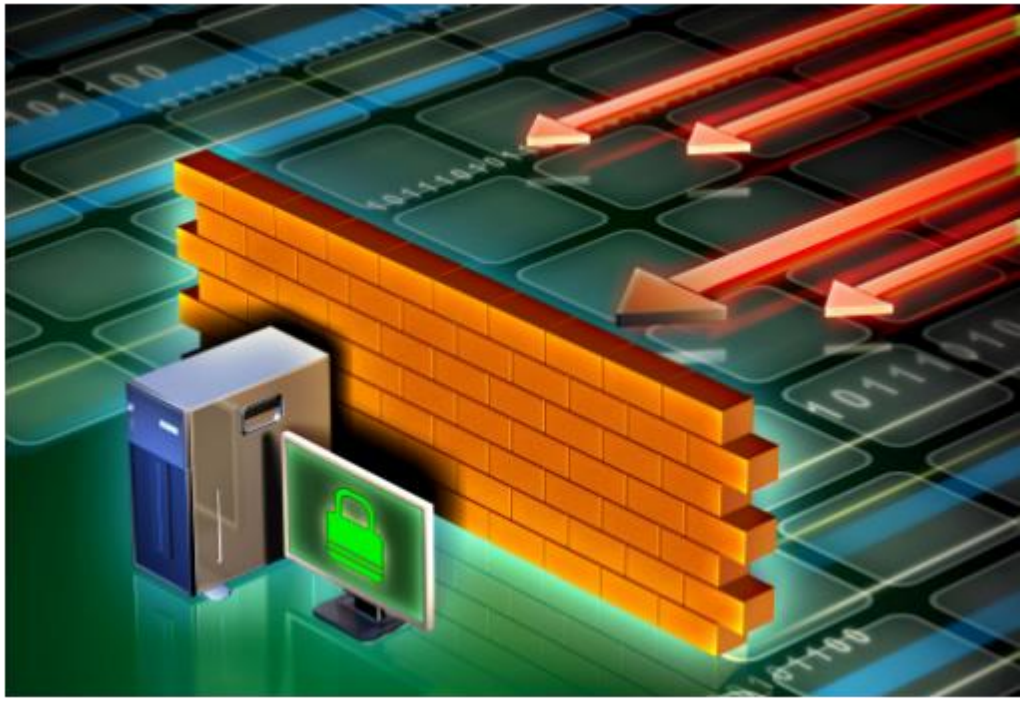


Майнинг, торренты, онлайн-игры

Устаревшее ПО

Отсутствие процедуры обновлений

КАК ПОЛУЧИТЬ ЧИСТЫЙ ИНТЕРНЕТ?



УСТАРЕВШИЕ СРЕДСТВА ЗАЩИТЫ НЕ СПОСОБНЫ ЗАЩИТИТЬ ВАШУ СЕТЬ ОТ ХАКЕРСКИХ АТАК

Kerio WinRoute Firewall

Traffic Inspector

UserGate

MikroTik

stonegate PUB COMPANY

Microsoft® Forefront™

Использование устаревших средств защиты сетевого периметра – причина 70% удачных кибератак.

КОНТРОЛЬ ПРИЛОЖЕНИЙ

ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ

UTM/NGFW

МЕЖСЕТЕВОЙ ЭКРАН

КОНТЕНТ-ФИЛЬТР

АНТИВИРУС ВЕБ-ТРАФИКА

АВТОРИЗАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

ПУБЛИКАЦИЯ РЕСУРСОВ

ИНТЕГРАЦИЯ В СЕТЬ

Шлюз

ИНТЕГРАЦИЯ В СЕТЬ

Прокси-сервер

IDECO UTM

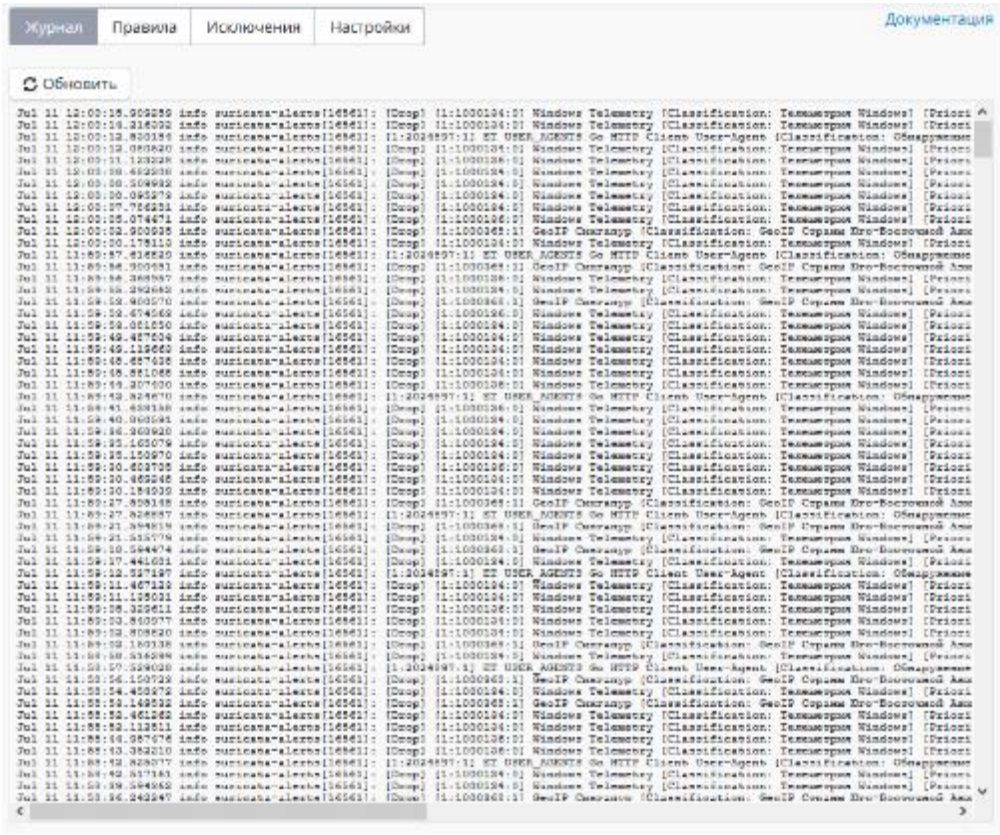
В 2 РАЗА

повышение эффективности
использования интернет-канала

2 ДНЯ

для внедрения в сеть

РЕЗУЛЬТАТЫ ЗА 1 НЕДЕЛЮ ПИЛОТНОГО ПРОЕКТА



	запросы	входящий, Мб	исходящий, Мб	блокировки
Онлайн-реклама и баннеры	35 939	158.51	30.94	35939
Черный список	18 283	80.47	18.03	18283
Технологии (в целом)	7572	33.34	10.67	7572
Анонимайзеры	7417	32.62	5.67	7417
Новости	1333	5.87	0.19	1333
Порнография	724	3.18	0.16	724
Взлом	365	1.60	0.24	365
Торрент-трекеры	123	0.54	0.06	123
Центры распространения вредоносного ПО	114	0.50	0.06	114
Казино, лотереи, тотализаторы	78	0.35	0.02	78
Видео для прослушивания и скачивания	72	0.32	0.03	72
Фишинг/мошенничество	68	0.30	0.03	68

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ!

Дмитрий Хомутов

d.homutov@ideco.ru

facebook.com/dhomutov

IDECO.RU