элефус

АКТУАЛЬНЫЕ ВЕКТОРА АТАК НА МЕДИЦИНСКИЕ ОРГАНИЗАЦИИ

О КОМПАНИИ

элефус

10 лет
НА РЫНКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ВЫПОЛНЕНО БОЛЕЕ **300** ПРОЕКТОВ

ПАРТНЕРСКИЕ СТАТУСЫ С ВЕДУЩИМИ ВЕНДОРАМИ РЫНКА ИБ

ЛИЦЕНЗИИ ФСТЭК И ФСБ РОССИИ

КОМАНДА СЕРТИФИЦИРОВАННЫХ ЭКСПЕРТОВ ПО РАЗЛИЧНЫМ НАПРАВЛЕНИЯМ

ЛИЦЕНЗИИ ФСТЭК И ФСБ РОССИИ


ЛИЦЕНЗИЯ
НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ


ЛИЦЕНЗИЯ

Критичные процессы

элефус

01 КОНФИДЕНЦИАЛЬНОСТЬ ОБРАБАТЫВАЕМОЙ ИНФОРМАЦИИ

В медицинских информационных системах обрабатываются персональные данные пациентов, медицинская информация. Необходимо соблюдать требования регуляторов по защите такой информации.

02 ОКАЗАНИЕ МЕДИЦИНСКИХ УСЛУГ

Врач с большой долей вероятности не сможет проконсультировать пациента по результатам анализов или исследований, если медицинская информационная система будет не доступна.

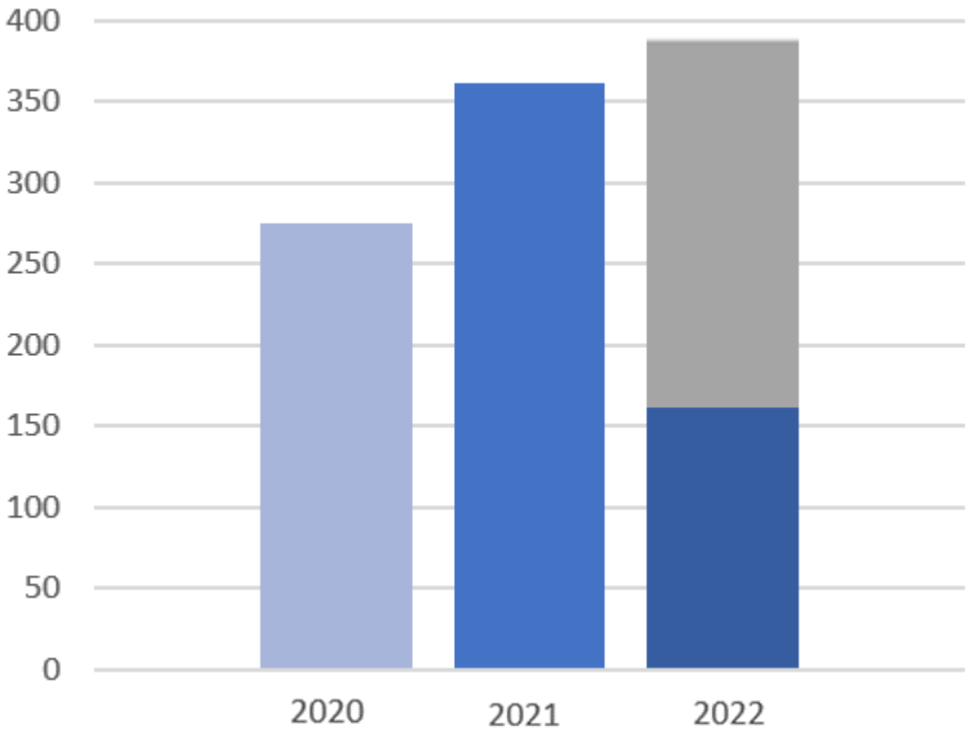
03 ДОСТОВЕРНОСТЬ ИСПОЛЬЗУЕМОЙ ИНФОРМАЦИИ

Медицинская информационная системы имеет интеграцию с лабораторной системой и другим медицинским оборудованием. Компрометация одной из систем может повлиять на работу другой.

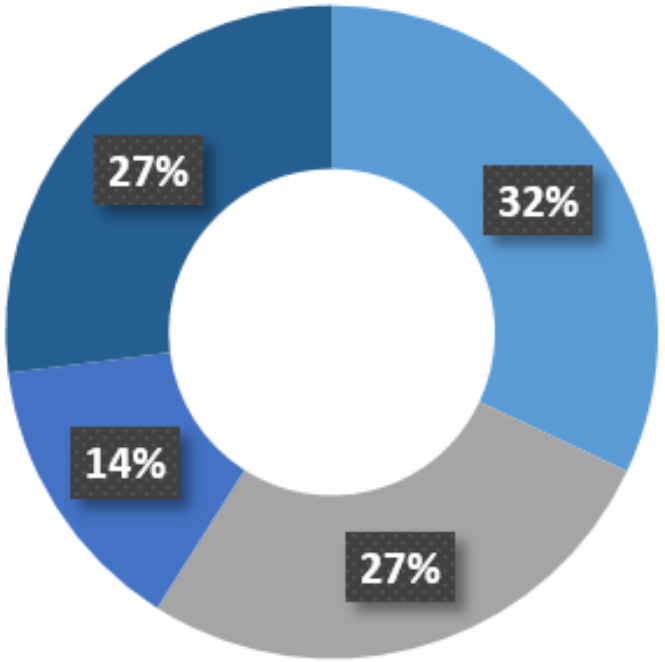
Статистика векторов атак

элефус

АТАКИ НА МЕДИЦИНСКИЕ ОРГАНИЗАЦИИ



ОСНОВНЫЕ ВЕКТОРА



Удаленный доступ Веб-приложения Фишинг Другие

КОМПРОМЕТАЦИЯ СЛУЖБ УДАЛЕННОГО ДОСТУПА

элефус

01

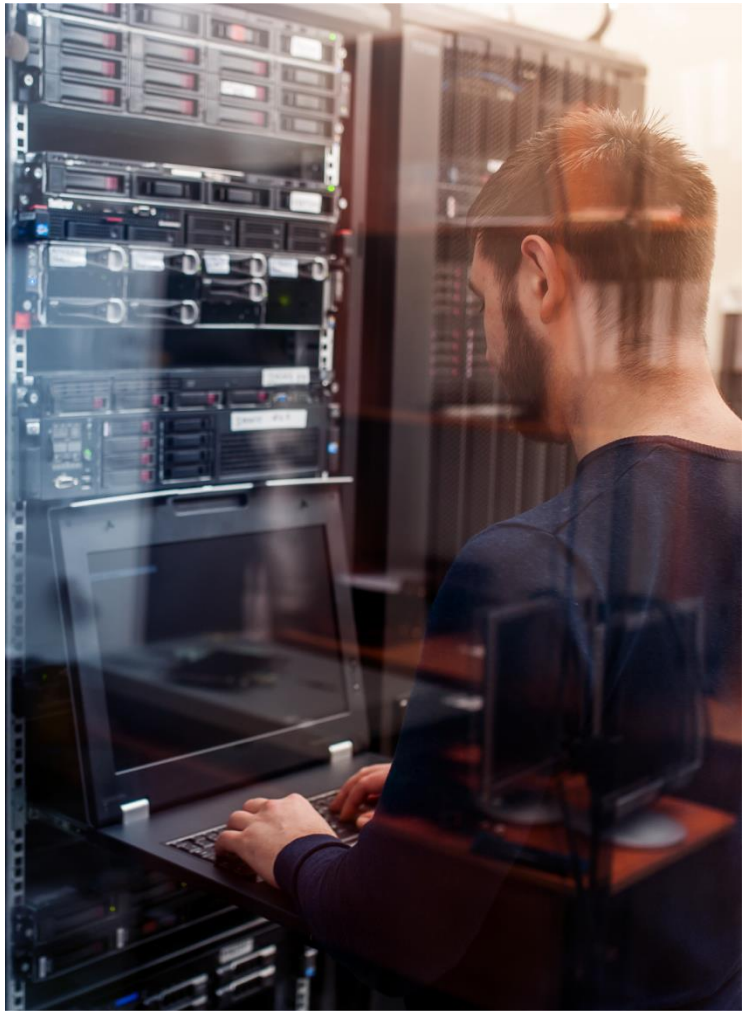
ПОЧЕМУ ЭТО ВОЗМОЖНО?

- не настроены списки доступа
- ошибочная публикация в сети Интернет удаленных сервисов
- уязвимости в используемых протоколах и ПО
- подрядчик имеет доступ к всему сегменту или сети

02

ЧТО МОЖНО СДЕЛАТЬ?

- введение «белых списков» IP-адресов
- VPN на базе лицензируемых решений
- блокировка невостребованных удаленных сервисов
- многофакторной аутентификации
- контроль действий подрядчиков



ЭКСПЛУАТАЦИЯ ПУБЛИЧНО ДОСТУПНЫХ ПРИЛОЖЕНИЙ

элефус

01 ПОЧЕМУ ЭТО ВОЗМОЖНО?

- автоматизация действий злоумышленников
- использование пользователями учетных данных
- уязвимости в бизнес-логике приложений

02 ЧТО МОЖНО СДЕЛАТЬ?

- ограничение числа попыток аутентификации
- проверка учетных данных в публичных утечках
- анализ кода веб-приложений
- использование межсетевых экранов уровня L7

ФИШИНГОВЫЕ РАССЫЛКИ

элефус

01 ПОЧЕМУ ЭТО ВОЗМОЖНО?

- использование корпоративных учетных данных на сторонних сайтах
- человеческий фактор
- отсутствие мониторинга действий пользователей

02 ЧТО МОЖНО СДЕЛАТЬ?

- запрет использования рабочей почты в личных целях
- повышение осведомленности пользователей
- автоматизация проверки писем в почтовых ящиках
- выявление подозрительного контента на уровне шлюза

ЗАКЛЮЧЕНИЕ

элефус

01 ОПРЕДЕЛЕНИЕ КРИТИЧЕСКИХ ПРОЦЕССОВ

Необходимо определить критические процессы именно для вашей организации.

02 АДАПТАЦИЯ ТРЕБОВАНИЙ РЕГУЛЯТОРОВ

Выполнение требований регуляторов по информационной безопасности, не только в части разработки документов, но и реализации мер.

03 ВЫСТРАИВАНИЕ ЭШЕЛОНИРОВАННОЙ ЗАЩИТЫ

Выстраивание эшелонов защиты для критических процессов в вашей организации.

Компания «Элефус»
г. Москва, Дербеневская наб. 11, корпус А

+7 (499) 653-63-17
sales@elephus.ru
www.elephus.ru