Безопасные бухгалтерские технологии.

Время войн в сфере ИТ. Как сохранить нервы, деньги и свое доброе имя.

+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

ЭПОХА БОЛЬШИХ ПЕРЕМЕН В СФЕРЕ ИТ

- Кардинальные изменения в операционных системах
- Удаленная работа вне офиса
- Виртуализация и контейнеризация
- «Облака» — суть чужие компьютеры
- Беспроводные устройства, «умные» устройства дома и в офисе

КАК ЭТО ВЛИЯЕТ НА НАШУ БЕЗОПАСНОСТЬ

- Хактивизм во всех видах
- Организованные APT-группы и массовый рынок уязвимостей нулевого дня
- Хакер-конструкторы и вредоносное ПО (malware), как бизнес-процесс
- Массовое использование методов социальной инженерии

УГРОЗЫ С ТЕХНИЧЕСКОЙ СТОРОНЫ

- Уязвимости нулевого дня
- Ошибки конфигурации
- Социальная инженерия
- Атаки на «цепочку поставщиков»
- Закрепление, повышение привилегий, боковое перемещение

УГРОЗЫ ПО СПОСОБУ РЕАЛИЗАЦИИ

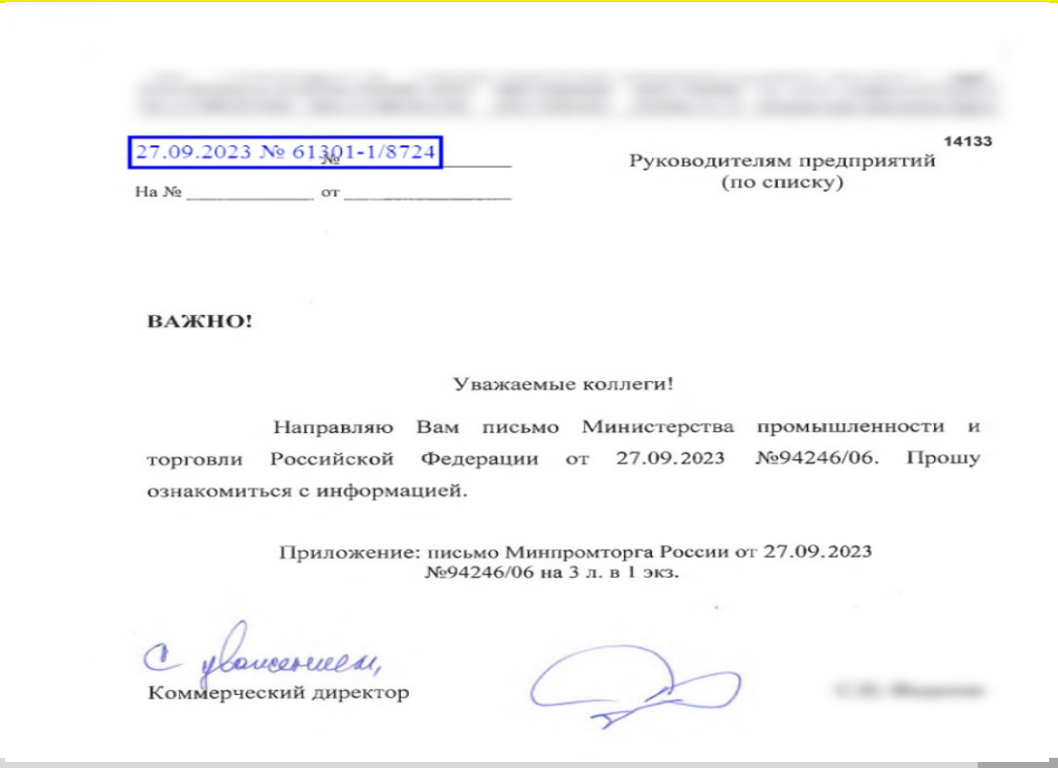
- «Ковровые бомбардировки»
- Удаленные «целевые атаки»
- Локальные «целевые атаки»

КАКИЕ ОПАСНОСТИ ПОДСТРЕГАЮТ БУХГАЛТЕРА

- Взлом рабочего компьютера
- Взлом домашнего компьютера
- Взлом мобильного устройства
- Фишинг (обман)
- Социальная инженерия (манипулирование)

ПРИМЕРЫ ИЗ ЖИЗНИ

- Фишинг. Mysterious Werewolf атакуют российскую электронную промышленность через уязвимость в WinRAR.
- Социальная инженерия. Приходит SMS с сообщением. Войти в учётную запись по ссылке, позвонит сотрудник безопасности.
- Кража денежных средств.
- 2023, октябрь. Атака на российское предприятие в сфере машиностроения.



27.09.2023 № 61301-1/8724
На № _____ от _____

14133

Руководителям предприятий
(по списку)

ВАЖНО!

Уважаемые коллеги!

Направляю Вам письмо Министерства промышленности и торговли Российской Федерации от 27.09.2023 №94246/06. Прошу ознакомиться с информацией.

Приложение: письмо Минпромторга России от 27.09.2023 №94246/06 на 3 л. в 1 экз.

С уважением,
Коммерческий директор

ПРИМЕР РАССЫЛАЕМОГО ВРЕДОНОСОГО ДОКУМЕНТА

ЗАЩИТА

- Здравый смысл и параноидальный подход
- Сети с нулевым доверием
- Виртуализация
- Терминальные серверы и фермы, VDI
- Тонкие клиенты
- Групповые политики
- SIEM,IDS, IPS

ПРАВИЛА БЕЗОПАСНОЙ РАБОТЫ

1. Работа без прав администратора
2. Политика ограниченного использования программ
3. Отключение неиспользуемых служб
4. Обновления
5. Брандмауэр
6. Резервное копирование
7. Антивирус

Если у меня стоит антивирус, я полностью защищен от вирусов?

— **Алексей Лукацкий**

бизнес-консультант по информационной безопасности Positive Technologies

вопрос эксперту

Если у меня стоит антивирус, я полностью защищен от вирусов?

Соответственно, полагаться на антивирус я бы не стал, и именно поэтому в базовых рекомендациях по ИБ для рядовых пользователей и корпораций **установка антивируса не входит даже в десятку защитных мер.**

Если у меня стоит антивирус, я полностью защищен от вирусов?

Если у вас стоит антивирус, то вы не защищены ни от чего. **Существует множество сервисов, которые позволяют проверить вредоносный код** на недетектируемость популярными антивирусами и средствами защиты конечных устройств.

А что говорит ChatGPT

Вот пять идей для безопасной удаленной работы бухгалтера из дома:

1. Использование защищенного VPN-соединения.
2. Двухфакторная аутентификация.
3. Регулярное обновление программного обеспечения.
4. Шифрование данных.
5. Регулярное резервное копирование данных.

И продолжает

Вот пять идей для безопасной работы бухгалтера в офисе:

1. Физическая безопасность.
2. Пароли и аутентификация.
3. Ограниченный доступ к информации.
4. Регулярное обновление программного обеспечения.
5. Обучение сотрудников.

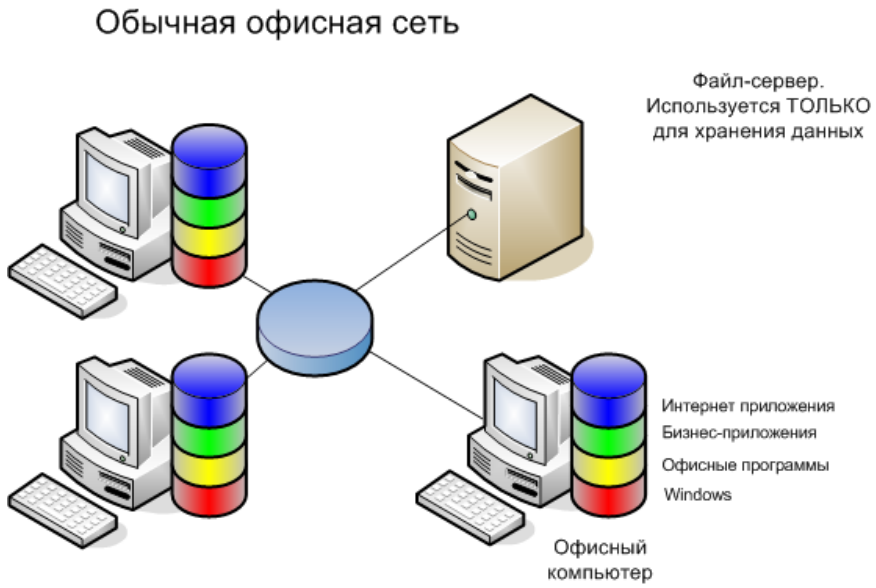
ДОПОЛНИТЕЛЬНЫЕ ОГРАНИЧЕНИЯ ДЛЯ УДАЛЁНЩИКОВ

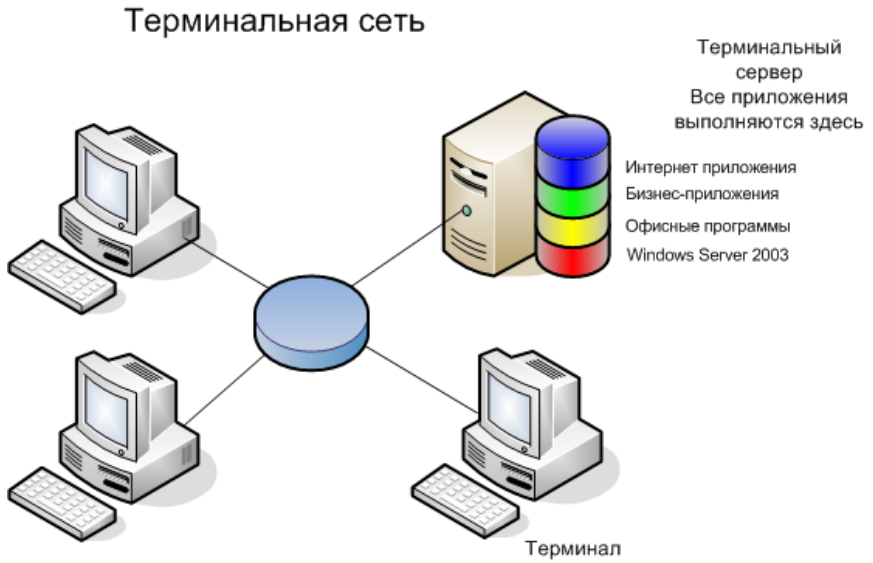
- Ограничения удаленного доступа по IP
- Сильные пароли
- Отключение виртуальных каналов в случае удаленного доступа по RDP

УМЕНЬШАЕМ ПЕРИМЕТР УЯЗВИМОСТИ

- Толстый клиент — дополнительная угроза
- Тонкий клиент — неизменяемый образ, минимальный размер
- Программное обеспечение для тонких клиентов — большой выбор
- Thinstation и его клоны
- WTware, Ponix, LTSP и т.д.

ТОЛСТЫЙ КЛИЕНТ VS ТОНКИЙ КЛИЕНТ





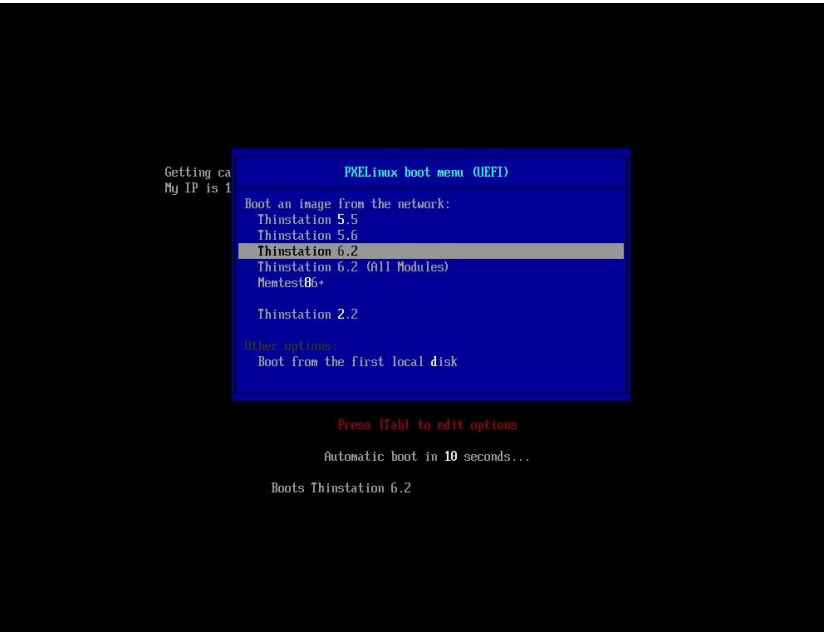
Thinstation — тонкий клиент с открытым исходным кодом

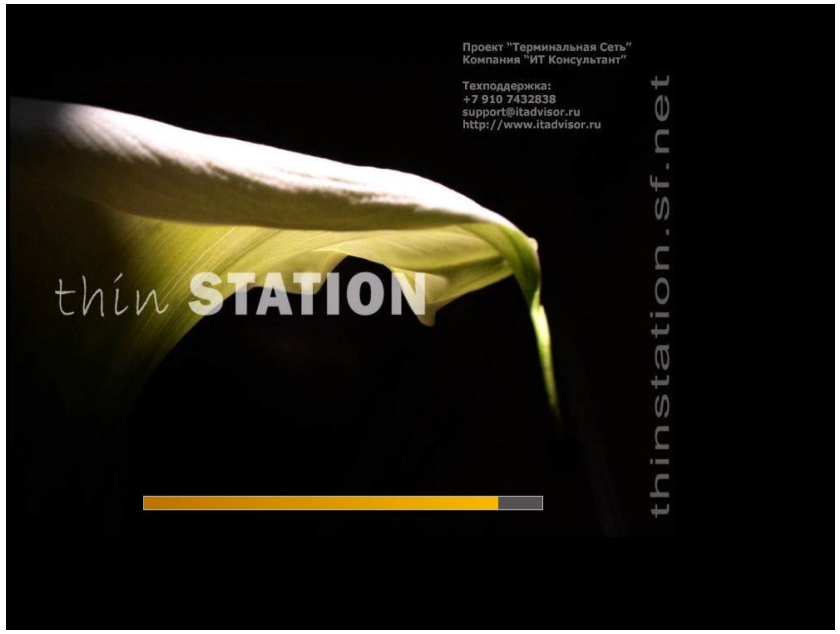
- Linux, основа — дистрибутив Crux Linux
- Открытый код
- Пересборка пакетов
- Добавляем свои пакеты
- Конфигурируем, как хотим

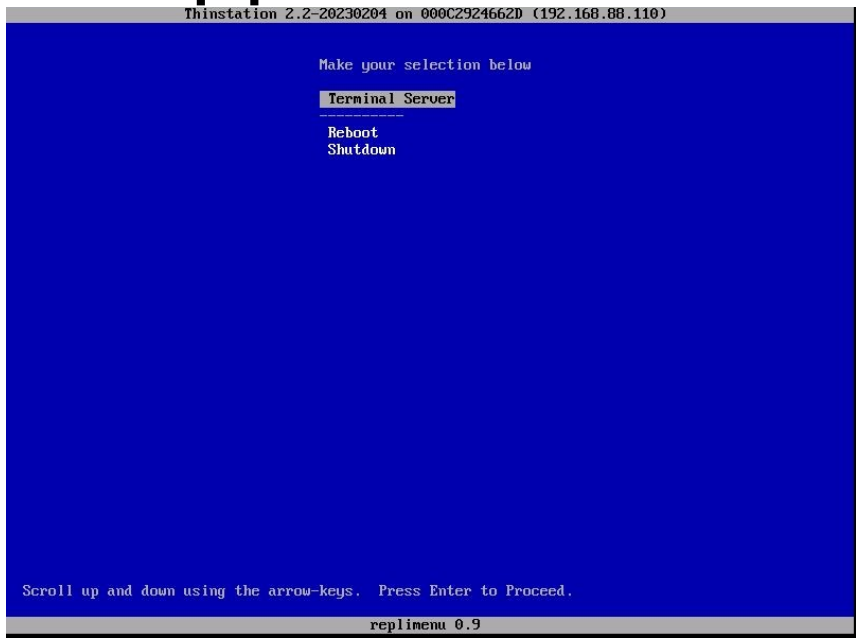
THINSTATION, КАК ЭТО УСТРОЕНО

- DHCPD
- TFTPD/HTTPD
- Pxelinux/ipxelinux
- Ядро
- Initrd
- Конфигурационные файлы + дополнительные пакеты

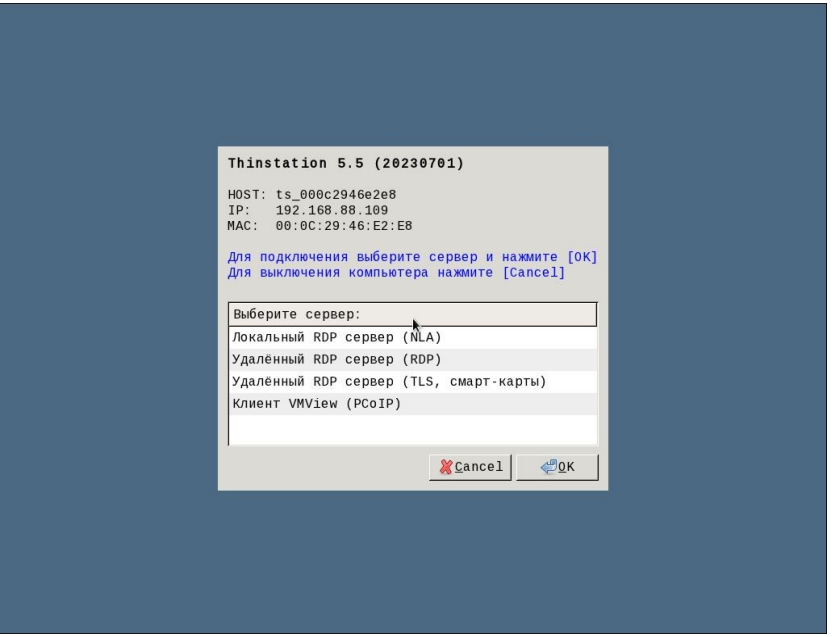
THINSTATION, КАК ЭТО ВЫГЛЯДИТ

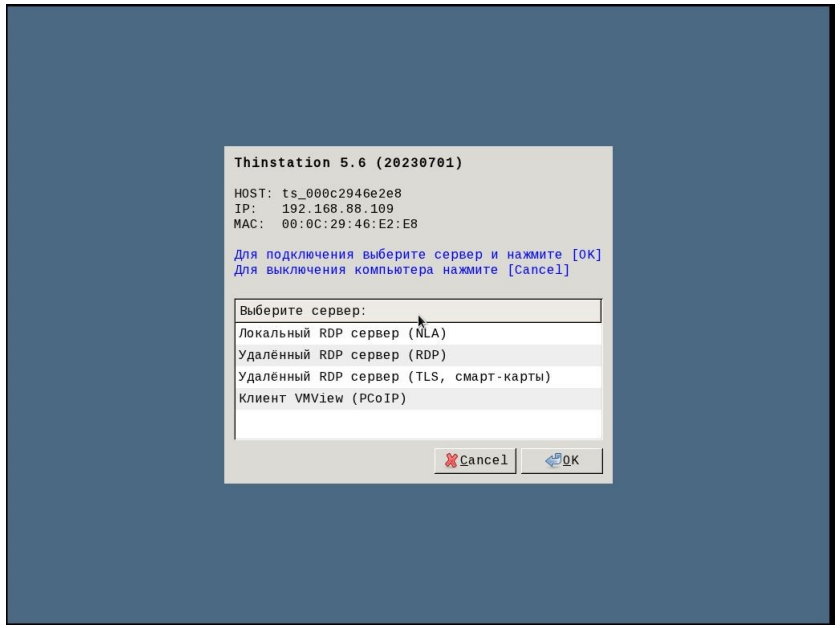


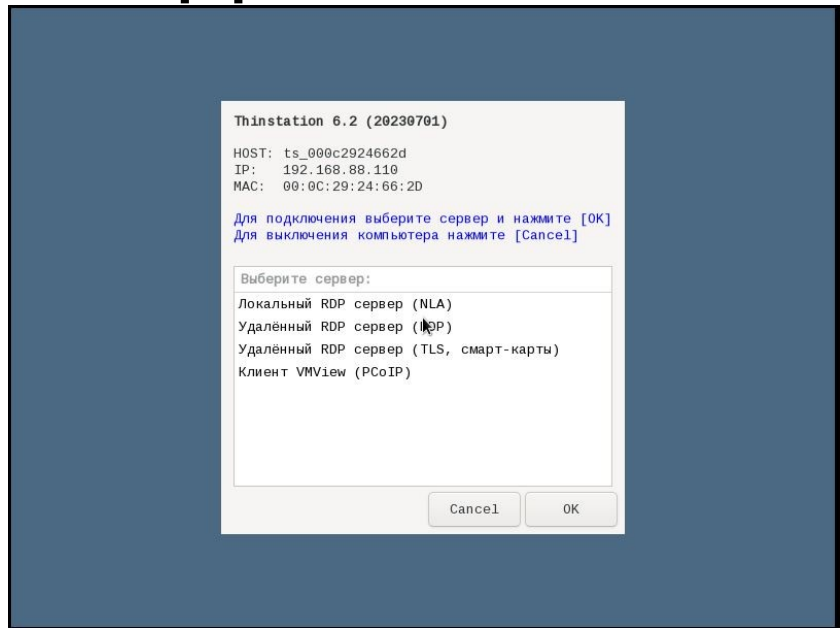




THINSTATION, КАК ЭТО ВЫГЛЯДИТ







THINSTATION, КАК ЭТО РАБОТАЕТ

- Загрузочные меню
- Конфигурационные файлы, виды сессий
- Поддержка RDS ферм
- Поддержка NLA

THINSTATION, В ЧЕМ ПРЕИМУЩЕСТВО

- Уменьшает периметр уязвимостей
- Поддерживает широкий спектр оборудования
- Продлевает жизненный цикл оборудования
- Нетребователен к ресурсам, загрузочный образ 30Мб
- Расширяем дополнительным функционалом
- Настраиваем чуть меньше, чем полностью

ЧТО ДЕЛАТЬ?

- Ревизия оборудования и используемых программных решений
- Составить список угроз
- Думать, принимать решения
- Готовы помочь

Ссылки в Telegram

Канал «Проект "Терминальная сеть"»

https://t. me/pts_itadvisor

Группа «Проект "Терминальная сеть"»

https://t. me/+j3PErS9wuVgzMDZi