ITSEC 2025

Конфлекс СПБ - это предприятие полного цикла по производству гибкой рулонной упаковки с печатью.
Мы работаем на рынке с 2001 года, имеем множество наград за качество выпускаемого продукта.

Наша упаковка сохраняет продукты и позволяет увеличивать их срок годности, поэтому от нашей работы зависит безопасность продуктов питания и товаров повседневного спроса.
В нашем портфеле заказов есть все продовольственные рынки и рынки товаров повседневного спроса, наши специалисты и технологи могут подобрать оптимальное решение под любой запрос.

Мы постоянно инвестируем в развитие и следим за тенденциями отрасли. У нас есть уникальное для российского рынка упаковки оборудование по нанесению лазерной высечки для придания упаковке дополнительных потребительских свойств.

В этом году мы приобрели пакетоделательное оборудование чтобы предложить партнёрам более широкий ассортимент продукции.
Так же мы можем наносить маркировку «честный знак», типографским способом, который обеспечивает надёжность кода и лучшую считываемость.

Объем выпускаемой нами продукции более 10 тысяч тонн в год.

Ленточкин Михаил.
Директор по информатизации ЗАО «Конфлекс СПб».

COMFLEX

ITSEC 2025

Наш опыт в организации уделённых рабочих мест. Практика

Удаленный доступ – тема широкая, но я планирую поделиться опытом реализации именно доступа по VPN к рабочим местам.

Задача

Организовать доступ к сервисам, своевременный, безопасный, контролируемый. Защита от не санкционированных подключений.

Основные сценарии:

- Удаленный доступ для внешних партнёров, к пром оборудованию (сервисмены и т.п.)
- Доступ для ключевых сотрудников, которые должны всегда быть на связи
- Доступ для не ключевых – ситуационный, временный
- Доступ для аварийных случаев, внезапный запрос

COMFLEX

ITSEC 2025

Самые простые решения, не правильные, опасные **(у нас конечно такого небыло)**
РДП наружу
VPN настроенный неизвестно когда и кем, для которого не менялись 100 лет пароли, который не стабилен.

В принципе, факторы риска
ПК пользователя, ПК с которого пользователь подключается в VPN может быть уязвим:

- Вирусы
- Гостевые доступы
- Отсутствие актуальных обновлений ОС, антивирусных баз
- Доступ третьих лиц (дети, муж, семья), кража или утеря устройства
- Стороннее ПО - VPN мужа для его работы, ПО детей, для посещения своих сайтов, игр в игры и т.д.
- Подключение с небезопасных площадок (WIFI в гостинницах часто даже пароли заводские не поменяны)
- Просто старый ПК, который еле еле работает (а ИТ получает сообщения, что «все неработает»)
- Неправильное использование ПК (рабочие файлы на домашнем рабочем столе, во время работы посторонняя активность, настройка шлюза ВПН – дефолтным шлюзом)
- «Уход» пароля от VPN третьим лицам, доступ к сохраненным на домашнем ПК паролям
- Доступ к ВПН с неизвестного, чужого устройства

Повысить безопасность технические меры:

1. Лучшая защита для ВПН – второй фактор.

минус второго фактора:

- Он сам не полностью безопасен (когда идет проверка, нужно ли запросить второй фактор, радиус-сервер отправляет данные для поиска учетной записи в АД – если эти запросы будут перехвачены и расшифрованы – это произойдет «изнутри» и эта атака окажется фатальной). Стоит позаботиться об это стороне вопроса.
- Часто сервис используемый для 2ФА является ИСПДН – надо помнить об этом.

2. При подключении к ВПН, доступ пользователя должен быть ограничен целевым ПК или сервером, как с помощью маршрутизации, так и на уровне фаервола.
3. Приобретение для ключевых сотрудников антивируса, обучение, установка ПО (ДЛП системы например и т.п.)
4. В ряде случаев, в некоторых странах хорошо себя показал протокол SSTP, т.к. прочие VPN блокировались.

Повысить безопасность организационные меры:

1. Процедура получения доступа по VPN – должна быть
2. Выдавать доступ нельзя бессрочно НИКОГДА.
3. Аудит с определенной периодичностью и подтверждение доступов. Если доступ не нужен – блокировать, «про запас» не оставлять доступы.
4. Анализ активности (не пользуется доступом, если пользуется – как пользуется, неудачные попытки подключения – все должно быть видно и доступно для анализа).
5. Пароли – менять, все пароли.
6. Необходимы некоторые базовые требования к оборудованию и программной среде пользователя, они должны быть сформулированы, утверждены и доведены до соответствующих лиц.
7. Проверка выполнения пункта 6 – регулярно.
8. Подписание соглашений о конфиденциальности

COMFLEX

ITSEC 2025

Некоторые найденные решения:

1. Домашний маршрутизатор – с настроенным ВПН, маршрутами, фаерволами

   Плюсы
   - Пользователь работает как работал, не думает о значке VPN, просто тыкает нужную кнопочку для подключения к своему рабочему столу.
   - Как ни странно, это не дорого
   - Устройство можно настроить, как только оно подключилось к VPN
   - Пользователь не знает лишние пароли, на ПК пользователя нет лишних маршрутов и прочих сущностей

   Минусы
   - Не всем подходит
   - Постоянно у пользователя, не удобно выдавать на короткий срок
   - Нельзя быстро изъять
   - Не взять в командировку

2. Служебный ноутбук

   Плюсы
   - Проверенное устройство, настроенное ПО
   - Пользователь может не знать пароли
   - Пользователь может не иметь своего ПК
   - Можно взять в командировку

   Минусы
   - Контролировать можно не всё, юсб порты, загрузка с флешек, даже запуск с другого жесткого диска – доступны.
   - В случае кражи, «Ломануть» проще чем роутер или флешку
   - Дорого

COMFLEX

Некоторые найденные решения: ITSEC 2025

1. Флешка загрузочная

   Плюсы

   - Пользователь не знает лишних паролей
   - Гарантированно Лицензионное, проверенное ПО
   - Зашифрованный образ – пароли не украсть
   - Привязка к ПК пользователя по паролю при загрузке – посторонний пользователь не загрузится с флешки
   - Нет лишних факторов, ничто не мешает работать (кино, ВКС, чужой софт)
   - Максимально лёгкий образ, летает даже на старинных ПК
   - Учет флешек = дополнительный контроль доступов к VPN

   Минусы

   - Не все устройства легко загрузить с флешки, даже ИТ-шникам
   - Сложность в настройке (первый интегратор – просто не сдюжил, второй – продавал готовый продукт со своей отечественной ОС – но по итогу наши ребята пол-года сами настраивали и исправляли баги)
   - Все равно нужна инструкция по VPN

COMFLEX

ITSEC 2025

Компетенции
Очень важно мотивировать коллег для расширения кругозора. Чтобы люди могли не просто «включить все нужные кнопочки» и ждать результат, а думали и повышали эффективность.

Специальное ПО, экономика
Глядя на цены ПО, особенно отечественного, может возникнуть желание, понаделать скриптов настроить все «как в интернет посоветуют» и много подобных идей по оптимизации затрат.

В реальности:
Тот же 2ФА, при настройке вручную, «съест» кучу времени вашего специалиста, передать это кому-то другому будет сложно, документацию проверить вы толком не сможете или потратите еще одну кучу времени.

Все это не сложно, но «съедает» достаточно много времени, чтобы при определенном объеме задач все же купить специально придуманное ПО. Просто купив ПО мы инвестируем, вместо зарплаты – в то, что останется в компании и будет работать долгие годы, будет обновляться, сертифицироваться, администрироваться и актуализироваться. Единственное, всегда уточняйте, что у Вас останется, когда вы перестанете платить, чтобы в одночасье не остаться совсем без сервиса.

Спасибо за внимание!!!