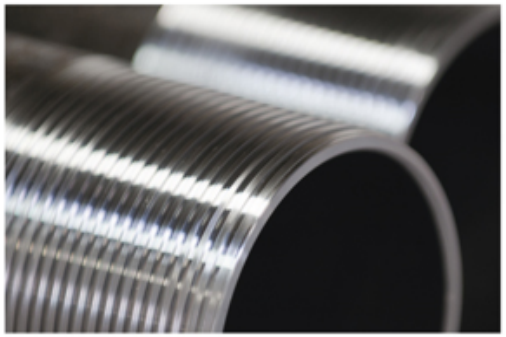
ТРУБНАЯ МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ



2020

Международный ТБ ФОРУМ Технологии Безопасности

ЧЕЛОВЕЧЕСКИЙ ФАКТОР В ИБ В УСЛОВИЯХ «УДАЛЕНКИ»

Подготовил: Севостьянов А.В.
Должность: Начальник Отдела защиты информации СЭБ
Город: Москва

Дата:02.07.20

Немного о проблемах и сложностях

Многим Компаниями надо было одномоментно: безопасно и оперативно вывести на удаленный режим работы массу работников – без существенной потери качества их работы!

Именно в этих условиях наиболее остро обозначились:

- **противоречия между IT и ИБ**
- **нехватка ресурсов (ПО, оборудование, сервисы)**
- **временная потеря качества управления процессами (куда бежать, что делать и надо срочно что-то придумывать)**
- **недостаточная компетентность персонала в вопросах ИТ и ИБ (дома нет HelpDesk, а офисе он может быть недоступен из-за перегрузки)**

Немного о рисках и угрозах

Расширяя возможности удаленной работы персонала со своих личных устройств (компьютер, ноутбук, планшет и смартфон), без превентивных мер безопасности, мы увеличиваем:

- риски утечек корпоративных данных (включая персональные данные, данные из СУБД, данные по разработкам и ноу-хау)
- риски проникновения в ИТ-периметр Компании вредоносного ПО
- риски спам- рассылок и фишинговых атак
- риски компрометации учетных данных пользователей (пары логин\пароль и т.д.)
- риски атак на критическую информационную инфраструктуру и системы клиент- банк
- риски утраты ключевой информации (e-token; сертификаты УКЭП)

Что не так?

Компания не имеет права требовать от работника содержать в цифровой чистоте свою личную компьютерную технику, а только рекомендовать! Поэтому, опасность для Компании представляет:

- наличие пиратских версий ПО и операционных систем
- устаревшие, не обновляемые и не безопасные версии ОС Windows
- отсутствие антивирусной защиты
- наличие скрытно функционирующего вредоносного ПО
- устаревшее и не безопасное коммуникационное оборудование (wifi-роутеры и т.д.)
- отсутствие у пользователя навыков безопасной работы (а в ряде случаев, не принятие подобной стратегии поведения)
- возможность печати служебных документов дома

Что делать? - 1

Организационный уровень:

- оперативное и масштабное проведение мероприятий «повышения осведомленности» (серии корпоративных вэбинаров; информационные рассылки, обучения) с подробными разъяснениями политики безопасной работы в удаленном режиме
- приобретение и выдача корпоративных ноутбуком персоналу (с предустановленным ПО защиты информациями; без прав администратора и минимально допустимым набором приложений для работы)
- определение схемы работы: кому ноутбуки; кому remote desktop access; как пускаем подрядчиков в ЛВС и кто остается в офисе с соблюдением санитарно-эпидемиологических мер
- организуем работу HelpDesk максимально оптимально (перераспределяем сервис только на поддержание критически важных систем и запросов)
- определяемся с двух факторной аутентификацией для УД

Что делать? - 2

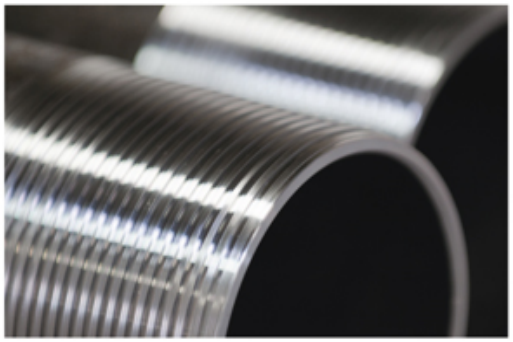
Прикладной уровень:

- усиливаем периметральную безопасность ИТ-инфраструктуры недостающими средствами и сервисами (расширяем пакет антивирусной защиты и firewall; дополнительные лицензии Microsoft для удаленной работы; обязательно ставим антиспам-фильтры на почтовый сервер)
- определяем ПО и сервис удаленного работы для подрядных организаций с фиксацией операций
- оперативно обновляем все типы операционных систем семейства Windows и сетевого оборудования (патч- менеджмент)
- организуем доступ персонала к общим папкам с разграничением доступа
- обеспечиваем безопасную работу критических систем: CRM, ERP, клиент- банк (эффективно: удаленный рабочий стол со служебного ноутбука, при этом - на дом работнику эталонное рабочее место не выдаем)
- определяем и разворачиваем контролируемый корпоративный сервис месседжинга и совместной работы (Ms. Teams и им подобные)

О контроле?

Применять DLP- системы и ПО контроля рабочего времени (включая модули антивирусных систем), принимает Компания по своему усмотрению, но с обязательным соблюдением действующего законодательства и на базе своих локальных нормативных актов!

Спасибо за внимание!



WWW.TMK-GROUP.COM