IBS Platformix

Актуальные вопросы информационной безопасности при организации гибридной работы сотрудников

Петр Старков

Руководитель отдела продуктового маркетинга
IBS Platformix

О чем пойдет речь?

Почему
IBS Platformix?

Что такое
гибридная работа?

Текущая ситуация

Угрозы
и **решения**

Выводы

IBS Platformix с 1992 на рынке корпоративных инфраструктур

Системный интегратор IBS Platformix с 1992 года успешно помогает предприятиям из различных отраслей создавать надежную платформу для ведения бизнеса.

Экспертиза интегратора направлена на реализацию типовых решений с необходимым и достаточным набором параметров.

2020 год:

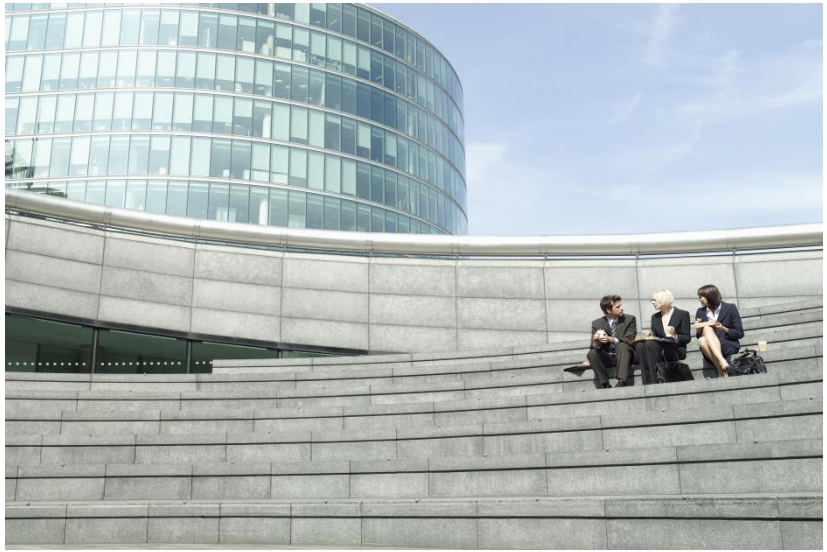
69 306
поставлено систем

381 937
инженерных часов

702
производителя

35
субъектов РФ

Гибридная работа – один из факторов риска



В России до 60% работников намерены и после пандемии полностью или частично работать удаленно*

В России удаленная работа менее популярна, чем в среднем по всему миру. Тем не менее большинство россиян предпочло бы и после пандемии не ездить в офис каждый день.

Согласно данным исследования, большинство респондентов предпочитают гибридную модель: два-три дня в неделю работать из дома, а остальное время - в офисе.

*Исследование BCG и The Network при участии HeadHunter, 2021

Особенности гибридной работы

На сегодняшний день большинство компаний уже имеют опыт организации удаленной работы:

- доступ к корпоративной сети при помощи VPN
- использование облачных сервисов
- применение мессенджеров и платформ для коммуникаций в режиме онлайн;
- увеличение количества устройств, которые подключаются к системам компании
- адаптация бизнес-процессов под новый формат

Как это влияет на безопасность?

Текущая ситуация. Угрозы

Об обеспечении безопасности гибридной работы задумываются не все…
Тем временем количество угроз растет:

- незащищенное соединение
- компрометация учетных записей сотрудников
- доступ в сеть с личных устройств с нелегитимными приложениями и ПО
- угроза удаленному устройству при отключении VPN
- разрозненные инструменты безопасности

Текущая ситуация. Решения

Как обеспечить защиту данных от угроз информационной безопасности вне зависимости от места работы сотрудника и расположения сервиса?

На рынке появляются инструменты, спроектированные с учетом особенностей гибридной рабочей среды и ориентированные на новые офисные пространства и новые типы пользователей.

Пример комплексных решений Cisco

Компания Cisco — мировой лидер в области информационных технологий, ведет свою деятельность с декабря 1984 г.

Доля Cisco на рынке в сетевом оборудовании 69% в коммутаторах и 37% в маршрутизаторах.

С 2013го года одним из главных фокусов стала Информационная Безопасность.

Угроза 1

Угроза:
незащищенное соединение

- несоответствие корпоративным требованиям к оконечным устройствам
- утечка конфиденциальных данных
- отсутствие защиты при сетевом подключении
- использование различных устройств при подключении к корпоративной сети

Решение:
VPN клиент с расширенными возможностями Cisco AnyConnect®

- единая система соответствия оконечных устройств нормативным требованиям
- защищенный сетевой доступ (IEEE 802.1x)
- обеспечение безопасности Web-трафика
- мониторинг сети (Модуль AnyConnect Network Visibility – контроль приложений)
- поддержка мобильных устройств

Угроза 2

Угроза:
компрометация учетных записей сотрудников

- использование ненадежных паролей
- подключение личных устройств к корпоративной сети
- использование устаревших и уязвимых устройств

Решение:
многофакторная аутентификация Cisco Duo

- проверка идентификационных данных пользователей
- оценка безопасности каждого устройства
- применение адаптивных политик для защиты доступа **к каждому приложению…** даже без VPN

Угроза 3

Угроза:
удаленному устройству при отключении VPN

- вредоносное ПО
- фишинг
- обратные вызовы командных серверов

Решение:
защита при отключенном VPN Cisco Umbrella

- включается автоматически при отключении VPN
- не требует никаких действий конечных пользователей
- защита от угроз по всем портам и протоколам
- дополнительные агенты не требуются. Достаточно включить поддержку Umbrella в клиенте Cisco AnyConnect
- средства мониторинга и управления на уровне DNS блокируют запросы на вредоносные домены и IP-адреса еще до установления соединения

Угроза 4

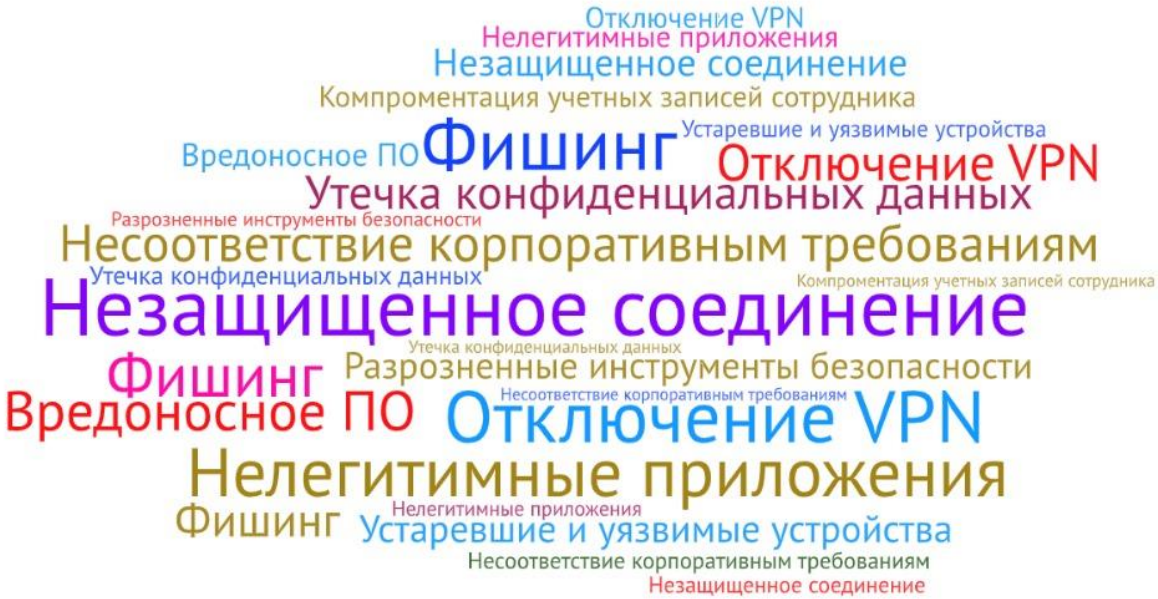
Угроза:
самому удаленному устройству

- вредоносное ПО
- фишинг
- обратные вызовы командных серверов

Решение:
защита класса EDR (Endpoint Detection & Response) Cisco Secure Endpoint

- защита Cisco от усовершенствованного вредоносного ПО
- блокирует атаки и помогает быстро и эффективно реагировать на угрозы
- изолировать зараженные хосты от остальной части сети
- сдерживать угрозу без потери данных для расследования
- сокращение затрат на восстановление за счет ограничения масштаба атаки
- быстрая реактивация конечной точки после завершения восстановления

Угроза #...


Отключение VPN
Нелегитимные приложения
Незащищенное соединение
Компроментация учетных записей сотрудника
Устаревшие и уязвимые устройства
Вредоносное ПО
Фишинг
Отключение VPN
Утечка конфиденциальных данных
Разрозненные инструменты безопасности
Несоответствие корпоративным требованиям
Утечка конфиденциальных данных
Компроментация учетных записей сотрудника
Незащищенное соединение
Утечка конфиденциальных данных
Фишинг
Разрозненные инструменты безопасности
Несоответствие корпоративным требованиям
Вредоносное ПО
Отключение VPN
Нелегитимные приложения
Нелегитимные приложения
Фишинг
Устаревшие и уязвимые устройства
Несоответствие корпоративным требованиям
Незащищенное соединение

Решение Cisco SecureX

Модульная система, в которую интегрируются все продукты Cisco для обеспечения безопасности.

SecureX помогает объединить всю вашу инфраструктуру безопасности для:

- **Автоматизация сбора инцидентов**
- **Автоматическая сортировка**
- **Интеллектуальная «склейка» в единые события**
- **Единый интерфейс расследования и реагирования.**

IBS Platformix & Cisco

Мы создаем инфраструктуру и разрабатываем решения для обеспечения информационной безопасности на всех участках предприятия:
от входа в здание до рабочего стола,
от портативного устройства до ядра системы.

Инсталляция, глубокие скидки за пакет решений, гарантия бесперебойной работы.

Предлагаем **комплекс решений** по **информационной защите** предприятия по семи направлениям:

- соответствие требованиям и стандартам
- консалтинг, аудит и анализ защищенности
- защита инфраструктуры и информационных систем
- аутентификация и управление доступом
- мониторинг и реагирование на инциденты информационной безопасности
- специализированные решения по защите информации
- безопасность разработки приложений

Спасибо за внимание!

Петр Старков

PStarkov@platformix.ru