

Вопросы кибербезопасности при удаленной работе в условиях COVID-19.

Илья Кравцов

Руководитель IBM Security в России и СНГ

Реакция на COVID-19 — Приоритеты ИБ при удаленной работе

Обеспечить непрерывность ИБ

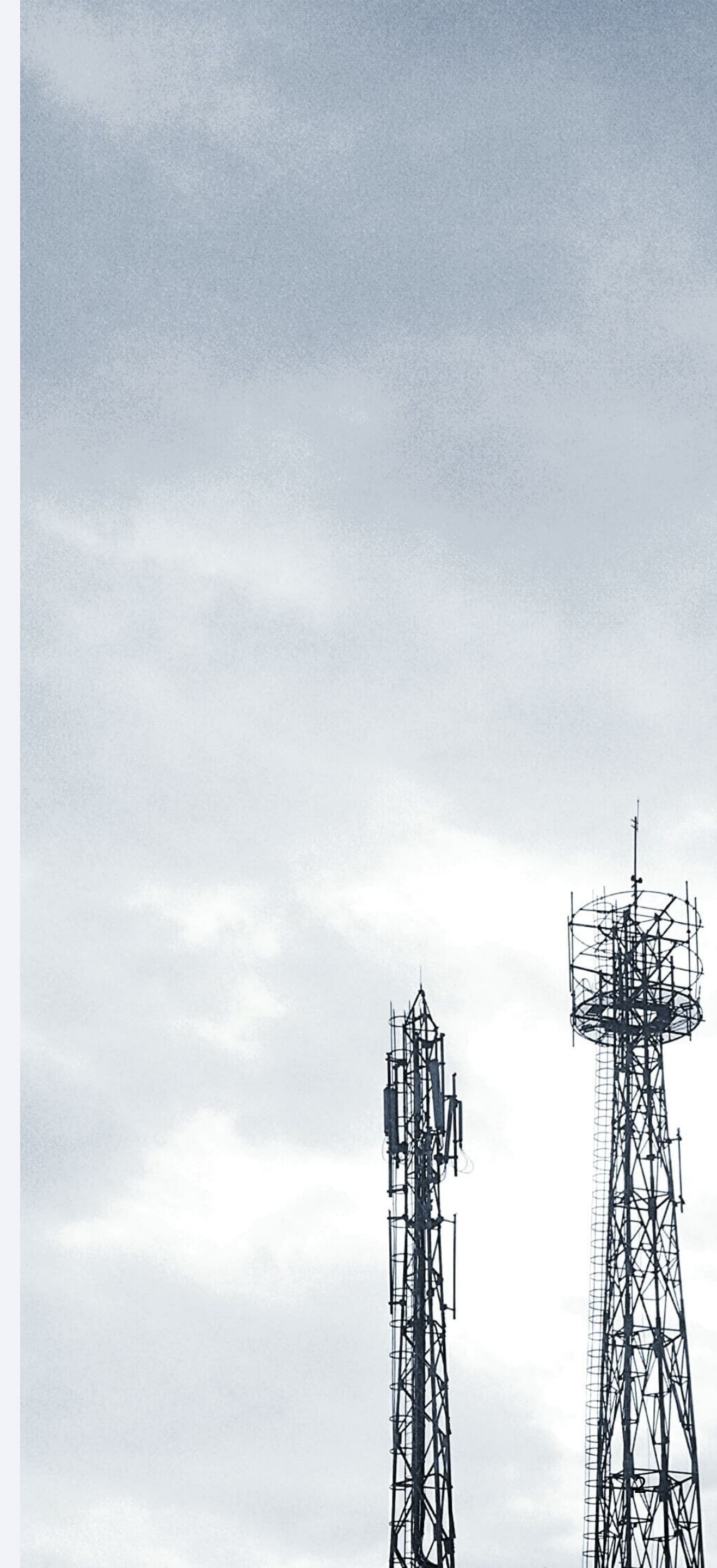
- Поддерживать работу службы ИБ в режиме 24/7
- Перейти на удаленное реагирование на инциденты

Быть готовым к новым угрозам

- Бдительность и осведомленность
- Обеспечить безопасность удаленной работы
- Понимать возросшие риски

Обеспечить готовность ИТ

- Определить критичные функции и сотрудников
- Обеспечить сотрудников необходимыми ресурсами
- Проработать план отказоустойчивости



Ограничения и риски удаленной работы

- У многих сотрудников нет защищенных корпоративных устройств
- Пропускная способность домашних сетей зачастую недостаточна для выполнения служебных обязанностей
- Масштабирование вычислительной инфраструктуры и поддержание ее в рабочем состоянии затруднены
- Резко возросшая нагрузка на корпоративные VPN-соединения
- Сотрудники используют домашние устройства, которые не защищены корпоративными средствами безопасности и контроля
- Неопределенность в вопросах соблюдения требований регуляторов



9

Рекомендаций для безопасной удаленной работы

1. Напомните сотрудникам о правилах безопасной работы из дома
2. Используйте корпоративные средства связи и совместной работы
3. Не используйте внешние сервисы для рабочих нужд
4. Пользуйтесь корпоративными устройствами для работы и соблюдайте политики безопасности
5. Будьте бдительны и помните о социальной инженерии
6. Соблюдайте гигиену нахождения в сети
7. Используйте двухфакторную аутентификацию
8. Обеспечьте необходимую пропускную способность VPN
9. Проводите тестирование на проникновение и безопасность приложений



Спасибо

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

© Copyright IBM Corporation 2020. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty, of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.