ИНФОЗАЩИТА
ITPROTECT GROUP

Защита информации во времена COVID-19

Факты

- **Brno University Hospital атакован 12 и 13 марта, в результате чего была остановлена его работа. Госпиталь имеет одну из крупнейших лабораторий по тестированию COVID-19 в Чехии.**

- **Рост СПАМа, связанного с COVID-19 более чем в 60 раз с момента объявления пандемии 11 марта 2020 (по данным IBM X-Force на 23.04.2020).**

- **Каждый день Gmail блокирует более 100 миллионов фишинговых писем. За последние недели примерно 18 млн. ежедневно связаны с COVID-19. (16.04.2020, https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond)**

Классификация атак

ИНФОЗАЩИТА ITPROTECT GROUP

По виду атак:

1. **Фишинг:**
   - **От лица известных организаций**
   - **От лица руководства компании-работодателей**
   - **От лица пользователей, пишущих в техподдержку**

2. Финансовое мошенничество

3. Вредоносные приложения для мобильных устройств

4. Атаки на WiFi

Классификация атак

По объекту атаки:

1. **На сотрудников переведенных на удаленку**
   (в частности, на руководящий состав)

2. На корпоративные сети

3. На «домашних» пользователей

Примеры атак

Несколько хороших обзоров с примерами:

- **Эксплуатация темы коронавируса в угрозах ИБ (Алексей Лукацкий)** https://habr.com/ru/company/cisco/blog/494726/

- **Как киберпреступники наживаются на пандемии COVID-19 — ТОП-7 способов (Олег Иванов)** https://www.anti-malware.ru/analytics/Threats_Analysis/How-Cybercrooks-use-COVID-pandemic-top-7

Списки атак связанных с COVID-19

Перечень различных атак с хронологией появления COVID-19 Cyber Attacks

https://www.webarxsecurity.com/covid-19-cyber-attacks/

Как защитить удаленные рабочие места

1. Корпоративная VPN
2. Двухфакторная аутентификация
3. Антивирусное ПО

Дополнительно

1. Решения класса MDM (разделение личных и рабочих данных)
2. Дополнительная защита на уровне шлюза
3. Системы повышения осведомленности сотрудников

Проблемы с персональными данными

1. Тотальный мониторинг, сбор данных со стороны государства

2. Мониторинг работы сотрудников на удаленке

Немного информации о нашей компании…☺

iTPROTECT GROUP

Мы обеспечиваем информационную безопасность наших заказчиков, и мы гордимся тем, что делаем это качественно.

Факты о компании

ИНФОЗАЩИТА ITPROTECT GROUP

СЕРТИФИЦИРОВАННАЯ СЛУЖБА
ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

60+
вендоров

40+
типов решений ИБ

350+
проектов

ЛИЦЕНЗИИ
ФСТЭК
ФСБ

2500+
клиентов в 2020 году

СЕРТИФИКАЦИЯ
ISO 9001
ISO 20000
ISO 27001
ГОСТ 54869-2011

УНИКАЛЬНЫЙ ОПЫТ

2008
год основания

300+
ДЕЙСТВУЮЩИХ СЕРТИФИКАТОВ В ОБЛАСТИ ИБ

Собственная исследовательская лаборатория

Основные решения…

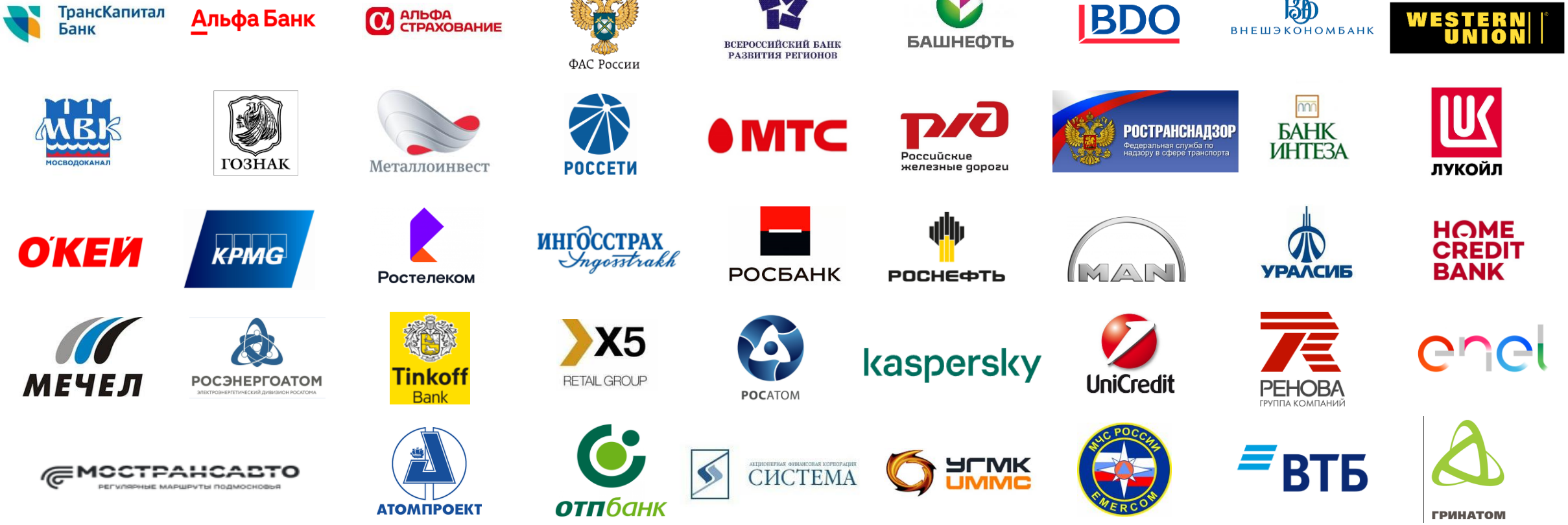
- Автоматизированное тестирование на проникновение PenTera
- Создание центров мониторинга безопасности (SOC/SIEM)
- Контроль действий привилегированных пользователей и ИТ-администраторов (PIM)
- Обеспечение информационной безопасности АСУ ТП и критической инфраструктуры (КИИ)
- Защита от направленных атак (APT/AET)
- Сетевая безопасность (NGFW/WAF/DDOS)

Основные решения

- Контроль устройств и шифрование данных
- Управление учетными записями (IDM)
- Защита мобильных устройств (EMM)
- Защита средств виртуализации и частных облаков
- Анализ безопасности кода приложений
- Системы защиты от утечек информации (DLP)
- Поведенческий анализ пользователей (UBA)
- Приманки и ловушки для хакеров - Deception

Нам доверяют

ИНФОЗАЩИТА ITPROTECT GROUP



Спасибо за внимание!

Евгений Вайман

Управляющий партнер

iTPROTECT GROUP

e.vayman@itprotect.ru

8-925-766-7999

Контакты:

Адрес: Москва, Дербеневская набережная, д.11, оф.502, БЦ «Полларс»

Тел./факс: +7 (495) 786-34-93; 7 (495) 120-64-46

www.itprotect.ru