Protection of corporate data in a remote working environment

Ilya Shalenkov
Head of Cyber Security and Digital Forensics, KPMG Russia and the CIS
January 2021

1. Access to the corporate network from personal devices

Lack of control of personal devices of employees who process corporate information

It is recommended to use solutions of the UEM (Unified Endpoint Management) class. Another option is to use the Virtual Desktop Infrastructure. In the short term – connecting the user's personal devices via VPN technology.

2. Transition to the Clouds

Fast transition to cloud solutions

It is recommended to conduct an independent audit of the existing cloud infrastructure. Do not forget about the compliance of cloud platforms with legal requirements. It is also recommended to think about solutions of the CASB – Cloud Access Security Broker class to solve the issues of monitoring the data exchange with cloud systems, as well as to connect them with existing information security event monitoring systems.

3. Lack of data leak control

Lack of systems for monitoring corporate data leaks

It is recommended to plan the implementation of the DLP – Data Loss Prevention system. Before implementation it is recommended to carry out an inventory of the available data and sources, to make sure that employees have access only to the information that they need for their work. It is also recommended to use regular monitoring means to detect suspicious activity in those systems, where possible.

4. Lack of cyberculture among users

Low employee awareness in information security

It is recommended to prepare information security memos/bulletins for employees on the conditions of remote work topic. You should pay attention to the issues of compliance with the principles of “clean desk” and “clean screen”, recommend security settings of the home Wi-Fi network, pay attention to the rules for creating passwords, warn against talking on the phone about work topics in the presence of unknown persons, etc.

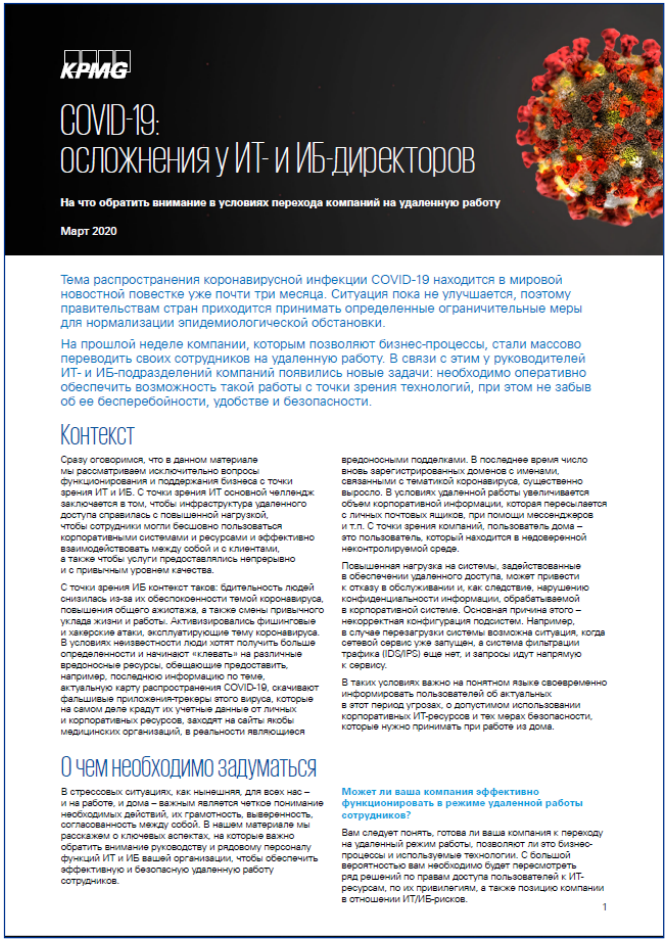
5. Lack of control of service providers

Lack of security controls for service providers / third parties

It is recommended to conduct an audit of service providers, including a thorough analysis of the processes and security tools they use to protect the transferred information. We also recommend using the services of proven suppliers.

COVID-19: difficulties for IT and IS directors

The article describes the key aspects which it is important to pay attention to the management and personnel of IT and information security functions of the company in order to ensure effective and secure remote work of employees.



KPMG

COVID-19:
осложнения у ИТ- и ИБ-директоров

На что обратить внимание в условиях перехода компаний на удаленную работу

Март 2020

Тема распространения коронавирусной инфекции COVID-19 находится в мировой новостной повестке уже почти три месяца. Ситуация пока не улучшается, поэтому правительствам стран приходится принимать определенные ограничительные меры для нормализации эпидемиологической обстановки.

На прошлой неделе компании, которым позволяют бизнес-процессы, стали массово переводить своих сотрудников на удаленную работу. В связи с этим у руководителей ИТ- и ИБ-подразделений компаний появились новые задачи: необходимо оперативно обеспечить возможность такой работы с точки зрения технологий, при этом не забыв об ее бесперебойности, удобстве и безопасности.

Контекст

Сразу оговоримся, что в данном материале мы рассматриваем исключительно вопросы функционирования и поддержания бизнеса с точки зрения ИТ и ИБ. С точки зрения ИТ основной челлендж заключается в том, чтобы инфраструктура удаленного доступа справилась с повышенной нагрузкой, чтобы сотрудники могли бесшовно пользоваться корпоративными системами и ресурсами и эффективно взаимодействовать между собой и с клиентами, а также чтобы услуги предоставлялись непрерывно и с привычным уровнем качества.

С точки зрения ИБ контекст таков: бдительность людей снизилась из-за их обеспокоенности темой коронавируса, повышения общего аффектажа, а также смены привычного уклада жизни и работы. Активизировались фишинговые и хакерские атаки, эксплуатирующие тему коронавируса. В условиях неизвестности люди хотят получить больше определенности и начинают «клевать» на различные вредоносные ресурсы, обещающие предоставить, например, последнюю информацию по теме, актуальную карту распространения COVID-19, скачивают фальшивые приложения-трекеры этого вируса, которые на самом деле крадут их учетные данные от личных и корпоративных ресурсов, заходят на сайты якобы медицинских организаций, в реальности являющиеся вредоносными подделками. В последнее время число вновь зарегистрированных доменов с именами, связанными с тематикой коронавируса, существенно выросло. В условиях удаленной работы увеличивается объем корпоративной информации, которая пересылается с личных почтовых ящиков, при помощи мессенджеров и т.п. С точки зрения компаний, пользователь дома – это пользователь, который находится в недоверенной неконтролируемой среде.

Повышенная нагрузка на системы, задействованные в обеспечении удаленного доступа, может привести к отказу в обслуживании и, как следствие, нарушению конфиденциальности информации, обрабатываемой в корпоративной системе. Основная причина этого – некорректная конфигурация подсистем. Например, в случае перезагрузки системы возможна ситуация, когда сетевой сервис уже запущен, а система фильтрации трафика (IDS/IPS) еще нет, и запросы идут напрямую к сервису.

В таких условиях важно на понятном языке своевременно информировать пользователей об актуальных в этот период угрозах, о допустимом использовании корпоративных ИТ-ресурсов и тех мерах безопасности, которые нужно принимать при работе из дома.

О чем необходимо задуматься

В стрессовых ситуациях, как нынешняя, для всех нас – и на работе, и дома – важным является четкое понимание необходимых действий, их грамотность, выверенность, согласованность между собой. В нашем материале мы расскажем о ключевых аспектах, на которые важно обратить внимание руководству и рядовому персоналу функций ИТ и ИБ вашей организации, чтобы обеспечить эффективную и безопасную удаленную работу сотрудников.

Может ли ваша компания эффективно функционировать в режиме удаленной работы сотрудников?

Вам следует понять, готова ли ваша компания к переходу на удаленный режим работы, позволяют ли это бизнес-процессы и используемые технологии. С большой вероятностью вам необходимо будет пересмотреть ряд решений по правам доступа пользователей к ИТ-ресурсам, по их привилегиям, а также позицию компании в отношении ИТ/ИБ-рисков.

1

KPMG

cyber@kpmg.ru

KPMG

Ilya Shalenkov

Director
Russia and CIS

Phone +7 (495) 937 44 77 (ext. 10138)
Mob. +7 (903) 792 80 77
Email ishalenkov@kpmg.ru

kpmg.ru