DOI 10.37882/2223–2966.2020.08.32

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ УДАЛЕННОЙ РАБОТЫ СОТРУДНИКОВ В УСЛОВИЯХ РЕЖИМА ПОВЫШЕННОЙ ГОТОВНОСТИ К ЧС

ENSURING THE SAFETY OF REMOTE WORK OF EMPLOYEES IN CONDITIONS OF HIGH EMERGENCY PREPAREDNESS

D. Suzdalsky

Summary. This research paper examines the main means of protection to ensure the security of remote access of employees of Aviaspectechnology LLC to information resources of the enterprise in the conditions of high emergency preparedness as a result of the SARS-CoV-2 pandemic.

In a high-alert mode, it is advisable to update information security threats to ensure remote access security, as well as introduce additional measures and means of information protection. In this regard, ensuring information security should be comprehensive, so it is advisable to apply a systematic approach that includes both technical and organizational measures.

The purpose of this work is to develop recommendations for organizations on reducing information security risks when forced to provide remote access to their employees. The impact of the high-readiness mode on the development of it technologies is also objectively assessed.

Keywords: SARS-CoV-2, COVID-19, coronavirus, remote access, high-alert mode.

Суздальский Дмитрий Андреевич
Российский Экономический Университет имени Г. В. Плеханова
t7699690@gmail.com

Аннотация. В данной научной работе исследуются основные средства защиты для обеспечения безопасности удаленного доступа сотрудников ООО «Авиаспецтехнология» к информационным ресурсам предприятия в условиях режима повышенной готовности к чрезвычайной ситуации в результате пандемии SARS-CoV-2.

В условиях режима повышенной готовности к чрезвычайной ситуации для обеспечения безопасности удаленного доступа целесообразно актуализировать угрозы безопасности информации, а также внедрить дополнительные меры и средства защиты информации. В связи с этим, обеспечение информационной безопасности должно быть комплексным, поэтому целесообразно применять системный подход, включающий в себя как технические, так и организационные мероприятия.

Целью работы является разработка рекомендаций для организаций по вопросу снижения рисков информационной безопасности при вынужденном предоставлении удаленного доступа своим сотрудникам. Также объективно оценивается влияние режима повышенной готовности на развитие ИТ-технологий.

Ключевые слова: SARS-CoV-2, COVID-19, коронавирус, удаленный доступ, режим повышенной готовности.

Введение

Режим повышенной готовности к чрезвычайной ситуации без преувеличения стал проверкой на прочность всех отраслей бизнеса. Поэтому, в условиях самоизоляции, организации в экстренном порядке реализуют для своих сотрудников удаленный доступ к своим информационным ресурсам, зачастую «закрывая глаза» на риски, связанные с информационной безопасностью.

SARS-CoV-2 содержит в себе угрозу не только жизни и здоровья людей, но и информационной безопасности в организации. Связано это со спешным переводом большинства работников различных предприятий на удаленный режим работы. До режима повышенной готовности к чрезвычайной ситуации большинство организаций, за исключением некоторых ИТ-компаний, не практиковало удаленный режим работы своих сотрудников, соответственно не было предусмотрено технологий, которые можно было бы масштабировать.

Компания ООО «Авиаспецтехнология» — агентство продаж авиа и ж/д перевозок. С 2003 года является Генеральным агентом авиакомпании «Ямал», география полетов которой постоянно расширяется и имеет обширную программу. Для удобства жителям и гостям Ямало-Ненецкого автономного округа агентство «Авиаспецтехнология» готово предоставить перечень услуг, которые не только позволят выбрать подходящий маршрут, но и сэкономить Ваше личное время. Спектр услуг постоянно обновляется. В агентстве можно:

- забронировать, узнать стоимость, купить авиабилеты, ж/д билеты выбрать подходящий маршрут или тур (туристические отделы);
- приобрести билет на аэроэкспресс;

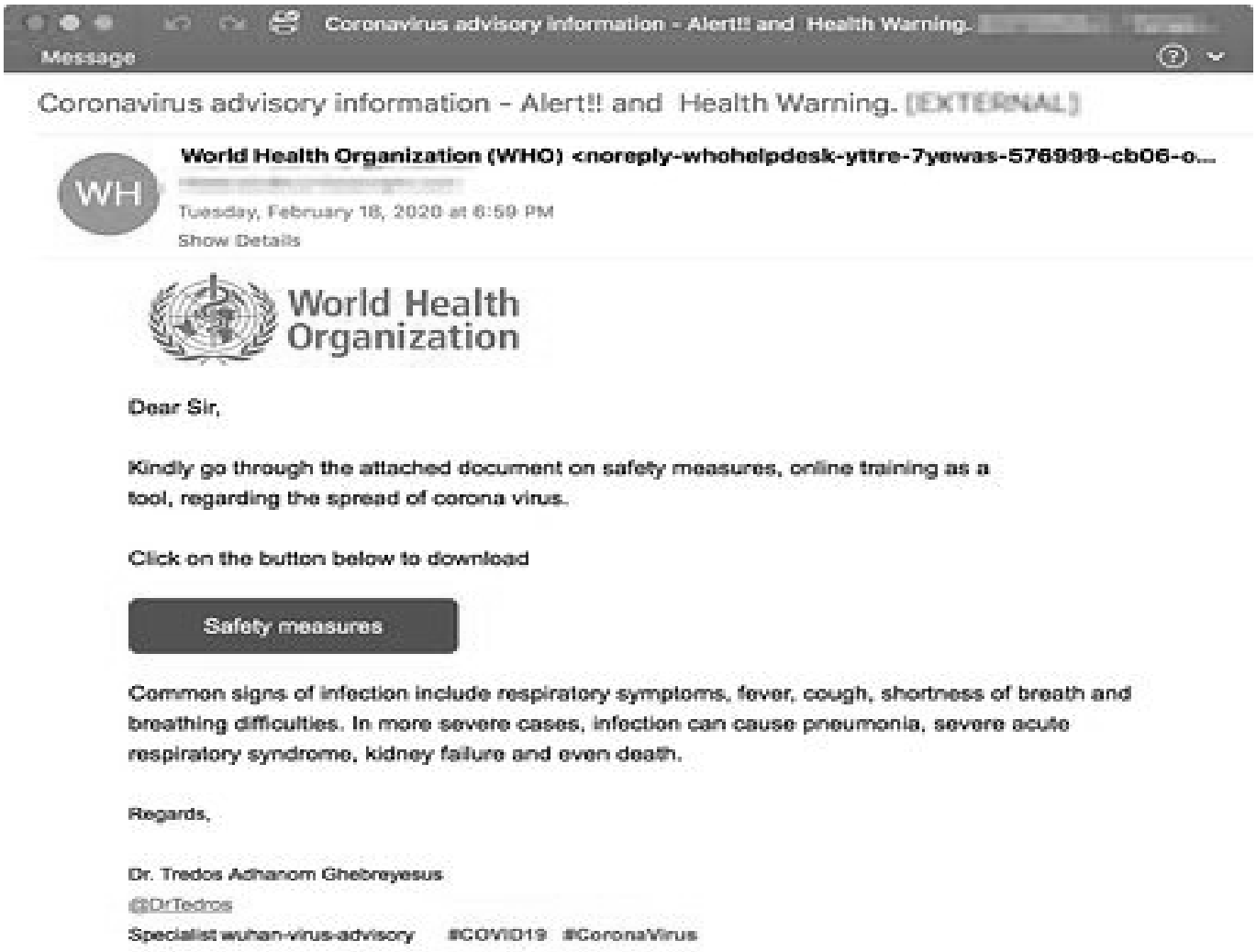

Рис. 1. Пример фишинговой рассылки якобы от имени ВОЗ

- забронировать гостиницу в любом городе;
- заказать трансфер (такси) и VIP- обслуживание в аэропортах страны (по запросу);
- оформить доставку почтовых отправлений;
- организовать деловую поездку по РФ и за рубеж (туристические отделы);
- заказать корпоративное обслуживание;
- выполнить чартерный рейс(чартер) на самолетах авиакомпании «Ямал» по вашим заявкам;

До введения ограничительных мер, ИТ-инфраструктура компании ООО «Авиаспецтехнология» удовлетворяла требованиям бизнеса. Однако, в условиях удаленной работы большого количества сотрудников серьёзно возросла нагрузка на ИТ-инфраструктуру ООО «Авиаспецтехнология». В связи с этим целесообразно проводить реинжиниринг процессов обеспечения информационной безопасности в условиях повышенных рисков ИБ, что и станет содержанием данной статьи.

Основная часть

При переходе на удаленный режим работы организация в свою копилку добавляет новые угрозы, некоторые из которых связаны с человеческим фактором, а некоторые с техническими аспектами предоставления удаленного доступа. При работе большинства работников через удалённый доступ, серьезно возрастает нагрузка на всю ИТ-инфраструктуру компании ООО «Авиаспецтехнология», в т.ч. на каналы связи, сетевое оборудование и т.д. В связи с данным фактом целесообразно осуществлять расширение интернет-канала, модернизировать сетевое оборудование на более производительные версии, пересмотреть технологии предоставления удаленного доступа в условиях повышенных рисков информационной безопасности.

В связи с режимом повышенной готовности к чрезвычайной ситуации информационная безопасность ак-

Рис. 2. Check Point Mobile для безопасного подключения к корпоративной сети

тивов требует значительно больше внимания, поэтому в должностные инструкции специалистов ИТ-отдела добавили функционал по обеспечению информационной безопасности удаленного доступа к корпоративным ресурсам компании ООО «Авиаспецтехнология».

В условиях режима повышенной готовности к чрезвычайной ситуации значительно увеличилось количество фишинговых атак на различные предприятия со стороны злоумышленников. Марк Роджерс, вице-президент компании Okta, работающей в сфере информационной безопасности, прокомментировал сложившуюся ситуацию: «*Я никогда не видел такого объёма фишинга. Я буквально вижу фишинговые сообщения на каждом известном человеку языке*» [1].

В условиях работы в режиме офиса работники предприятия осуществляют свою деятельность в рамках действующих регламентов и процедур по обеспечению информационной безопасности. Находясь вне офиса, работники организации могут не задумываться о новых угрозах, связанных, например, с перехватом данных, передающихся по незашифрованному каналу. Большинство работников предприятия, в условиях удаленного доступа, используют свои устройства для доступа к корпоративным ресурсам. Соответственно злоумышленники, в свою очередь, могут эксплуатировать уязвимости домашнего роутера работника организации с устаревшей прошивкой и дефолтной связкой логин-пароль «admin-admin». В рамках отсутствия у большинства компаний концепции BYOD для безопасного доступа с мобильных устройств и иных политик и технологий удаленного доступа, которые могли бы быть масштабированы в условиях режима повышенной готовности к чрезвычайной ситуации, потребовался реинжиниринг процессов обеспечения информационной безопасности. В связи с этим, проанализируем основные средства защиты, внедрение которых поможет снизить риски информационной безопасности для «неподготовленных» компаний. Целесообразно внедрять нижепредставленные решения:

1. Компания Check Point предлагает в течение 2-х месяцев бесплатно использовать собственные решения в области организации удаленного доступа.

С использованием Check Point Mobile возможно подключение с домашнего устройства к корпоративной сети по защищенным технологиям SSL VPN и IPSec VPN [2].

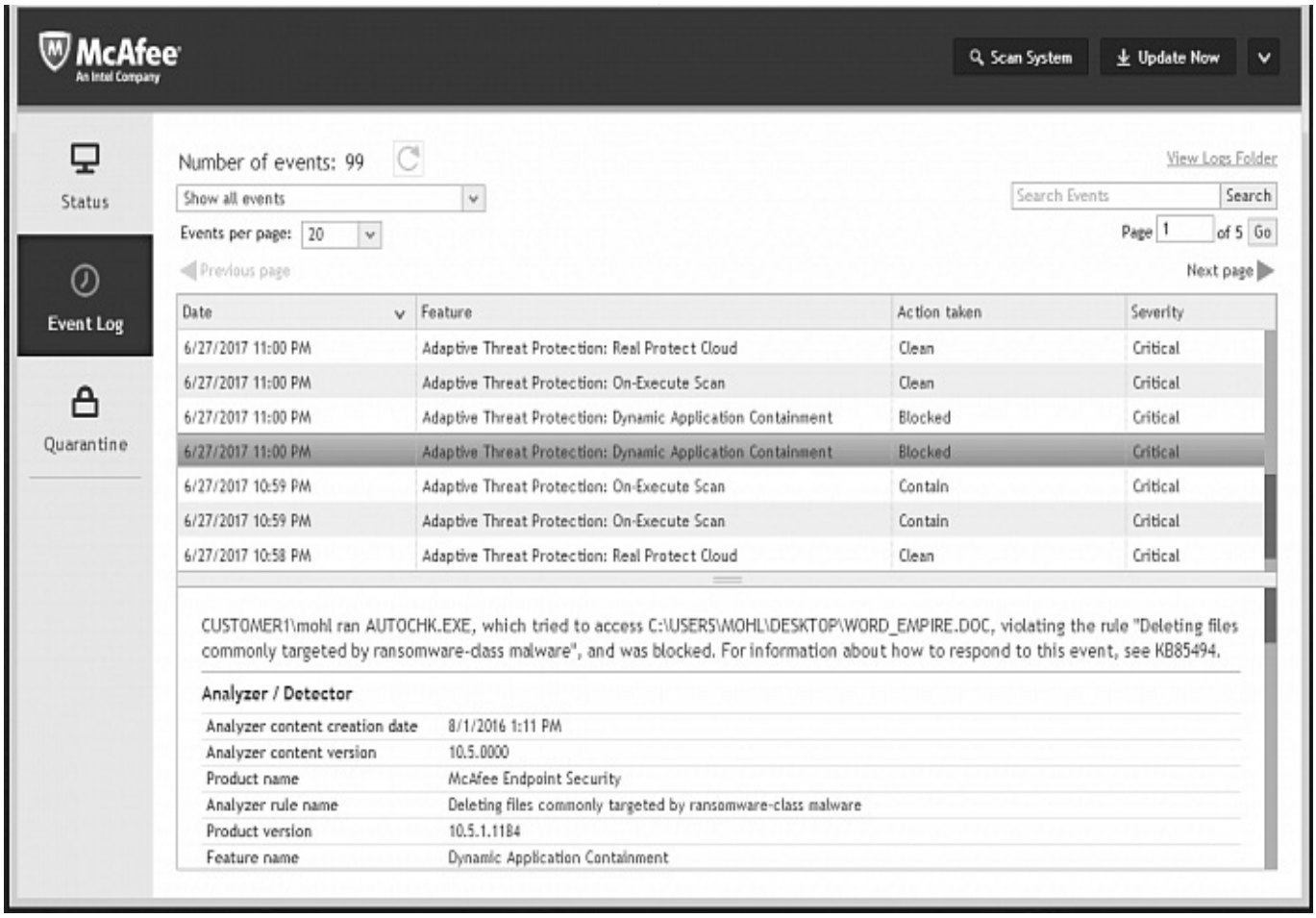

Рис. 3. Защита личных ПК с использованием антивирусного ПО McAfee

Для доступа сотрудников из отдела Бухгалтерии организован удаленный доступ к корпоративным ресурсам ООО «Авиаспецтехнология» с использованием технологии IPSec VPN. После подключения к локально-вычислительной сети, сотрудник организации при помощи RDP-сеанса подключается к своей рабочей станции. До реинжиниринга процесса удаленной работы, удаленный доступ, в случае разовых задач, либо отчётного периода, предоставлялся через программное обеспечение TeamViewer.

2. Организация McAfee предоставляет организациям возможность обеспечить бесплатную защиту персональных устройств удаленных сотрудников в срок до 31 мая 2020 года. К бесплатным продуктам, в условиях режима повышенной готовности, относятся [3]:

- McAfee Complete Endpoint Protection;
- McAfee Complete Data Protection

При установлении VPN-соединения, личные компьютеры работников предприятия также становятся частью информационной системы организации, и должны быть защищены надлежащим образом. Для обеспечения защиты рабочих станций сотрудников в ООО «Авиаспецтехнология» используется антивирусное программное обеспечение McAfee. До реинжиниринга процессов в компании ООО «Авиаспецтехнология», при предоставлении удаленного доступа через программное обеспечение TeamViewer, антивирусная защита пользовательских компьютеров никак не отслеживалась и не регламентировалась.

3. Организация Okta предоставляет организациям бесплатные решения для безопасной идентификации пользователей — систему с единой точкой входа (SSO), а также приложение для многофакторной аутентификации работников (MFA) на шестимесячный срок [4].

Для работы с приложениями корпоративной сети в условиях удаленного доступа необходимо наличие единой точки входа с различных устройств. В связи с этим, в компании ООО «Авиаспецтехнология» внедрено решение SSO от компании Okta. До реинжиниринга процессов обеспечения ИБ, в компании ООО «Авиаспецтех-

Рис. 4. Единая точка входа к приложениям с использованием ПО SSO Okta.

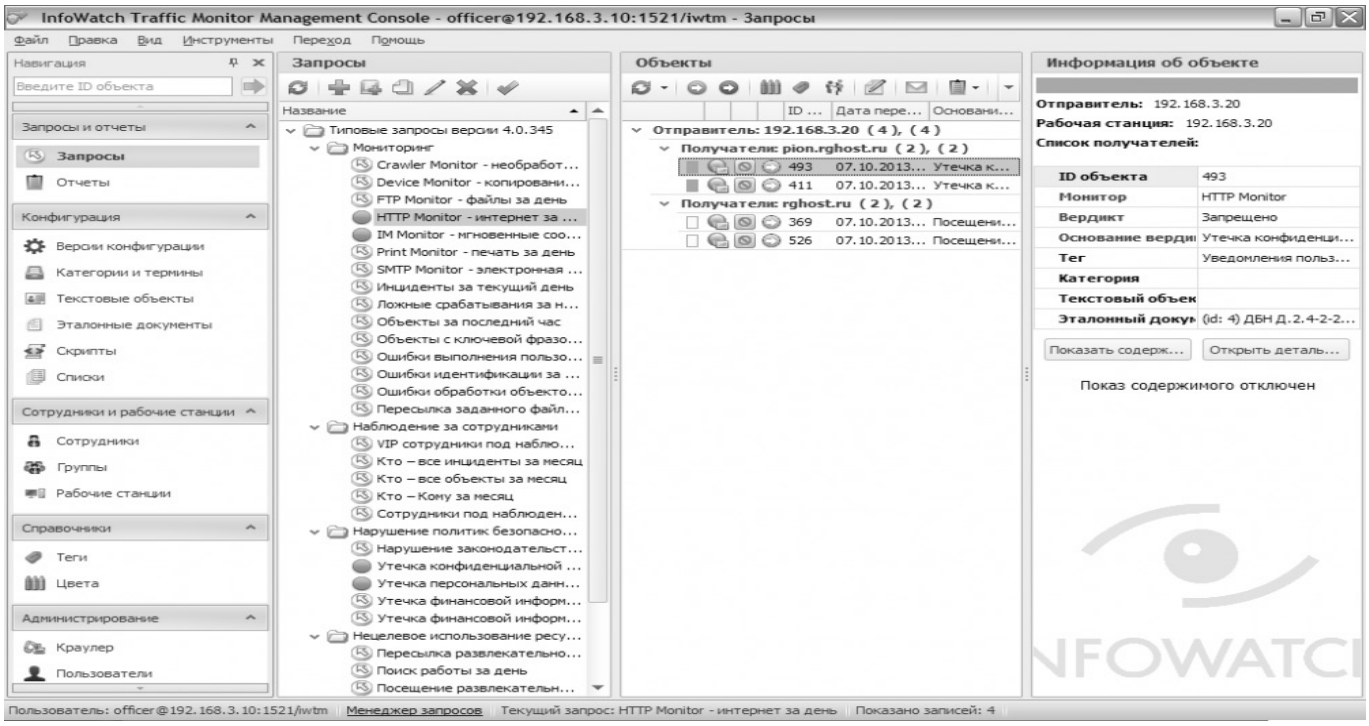

Рис. 5. Контроль удаленных пользователей.

нология» отсутствовала единая точка для доступа к приложениям. При необходимости работы с тем, или иным приложением через удаленный доступ, сотрудник организации, с использованием программного обеспечения TeamViewer, подключался к рабочей станции, откуда и работал с конкретным приложением. В новом варианте работы достаточно с домашнего компьютера подключиться к нужному приложению с использованием технологий компании Okta. При этом не требуется удаленное VPN-подключение к компьютеру, что снижает нагрузку на ИТ-инфраструктуру ООО «Авиаспецтехнология».

4. Российская компания ЗАО «Инфовотч» запустила акцию «Anti-COVID» [5], которая заключается в бесплатном месячном предоставлении системы InfoWatch Person Monitor, контролирующей действия удаленных сотрудников.

Учёт действий сотрудников ООО «Авиаспецтехнология» производится при помощи программного обеспечения InfoWatch Person Monitor с добавлением статистики в InfoWatch Traffic Monitor.

До реинжиниринга процессов ИБ детальный учёт действий пользователей не фиксировался.

Использование бесплатного программного обеспечения является целесообразным, учитывая финансовые расходы организации в связи с режимом повышенной готовности к чрезвычайным ситуациям, вызванным пандемией SARS-CoV-2. В связи с этим, специалистами ИТ-отдела ООО «Авиаспецтехнология» внедрены вышеуказанные средства защиты информации с целью минимизации затрат на введение режима удаленной работы.

Заключение

На мой взгляд, режим повышенной готовности к чрезвычайной ситуации в определенной степени послужит дополнительным стимулом к развитию рынка решений по информационной безопасности. В связи с этим, большинство организаций, имея возможность получить бесплатный доступ к средствам защиты информации от ведущих вендоров, оценив их эффективность, примет решение приобрести в дальнейшем те или иные средства защиты информации, в т.ч. и средства контроля своих сотрудников. Безусловно, текущая ситуация является трудной для большинства организаций, однако, с помощью крупных ИТ-компаний у них имеется возможность минимизировать риски информационной безопасности.

ЛИТЕРАТУРА

1. 3dnews [Электронный ресурс]. — Режим доступа: https://3dnews.ru/1007038
2. Официальный сайт компании CheckPoint [Электронный ресурс]. — Режим доступа: https://www.checkpoint.com/products/mobile-access/
3. Официальный сайт компании McAfee [Электронный ресурс]. — Режим доступа: https://www.mcafee.com/enterprise/ru-ru/products/endpoint-security.html
4. Официальный сайт компании Okta [Электронный ресурс]. — Режим доступа: https://www.okta.com/products/single-sign-on/
5. Официальный сайт компании ЗАО «Инфовотч» [Электронный ресурс]. — Режим доступа: https://www.infowatch.ru/

Журнал «Современная наука: актуальные проблемы теории и практики»