leowolfert © 123RF.com

Цифровая безопасность госслужащего

В век продвинутых технологий по-прежнему крайне высока личная беспечность пользователей устройств с доступом в интернет. И если внутренние сети и стационарные компьютеры защищены, то брешь легко пробивается через личную технику. Госслужащие не исключение. А в условиях удаленной работы риски возрастают.

Береги секреты

В 2018 году аудиторско-консалтинговая группа PwC обнародовала данные опроса топ-менеджеров российских компаний: 81% членов советов директоров хранят закрытую и дорогостоящую информацию на своих телефонах, а 29% опрошенных предпочитают общаться с другими членами советов директоров с помощью личной электронной почты. Аналогичных данных по госслужащим, в том числе чиновникам высокого регионального и федерального ранга, нет.

Оговоримся: в текущей ситуации удаленной работы условно можно классифицировать госслужащих на тех, кому необходимы усиленные меры кибербезопасности в связи с родом работы, и на остальных. Причем данное разделение не всегда зависит от должности, но и от того, к каким данным по роду своей деятельности человек имеет доступ и каким законом те охраняются (Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и др.). В зависимости от этого существуют регламентированные требования по защите или по устройствам, которыми должны пользоваться чиновники. И в принципе эти требования не будут отличаться, удаленно работают люди, у которых есть доступ к определенному типу данных, или нет.

В остальном в условиях массовой удаленной работы единого свода правил по информационной безопасности сейчас нет. Поэтому каждое ведомство исходит из своей практики. Кто-то выдает пользователям для удаленной работы корпоративные устройства с уже настроенным механизмом шифрования и разрешает пользоваться только ими. Кто-то разрешает работу с личных устройств, установив требования, которые должны соблюдаться (пароль на загрузку операционной системы, наличие на устройстве антивирусной программы с актуальными базами, хранение информации на отчуждаемом USB-носителе и т. д.). Регламентируется сложность паролей, способы обмена информацией (например, архивирование с паролем при пересылке), регламентируется собственно перечень информации, которую можно переда-

вать (например, запрещена передача информации для служебного пользования и информации, содержащей персональные данные). Проблема в том, что зачастую люди не отдают себе отчет в том, какую информацию они обрабатывают — рабочая рутина для одних может являться коммерческим интересом для других.

— Госслужащие должны быть, что называется, профессиональными параноиками, потому что работают с критичной для утечки информацией, имеют доступ к значимым ресурсам. В крупных организациях и компаниях ИБ-специалисты разрабатывают политику безопасности (что можно и нельзя делать на рабочем месте с информацией), разграничивают уровни доступа, контролируют коммуникации и движение файлов (для этого устанавливают IDS/IPS-решения, DLP, SIEM-системы, программы файлового аудита и другие). Если следовать их указаниям, риски потерять информацию сводятся к нулю. Но всегда сохраняется угроза, что сотрудник станет жертвой социнженера — откликнется на манипуляцию, установит вредоносное ПО или произведет опасные действия, — рассказывает **А. Б. Парфентьев**, руководитель отдела аналитики «СерчИнформ».

Другая, более обширная проблема — использование личных устройств, в первую очередь смартфонов. Из-за удобства их используют повсеместно, но проблема в том, что защищены они в разы хуже корпоративных. При этом ставить в известность работодателя о приобретении таких гаджетов в целях обеспечения информационной безопасности нет оснований. Сама по себе обязанность не разглашать соответствующие сведения зафиксирована должностными регламентами, соблюдение которых в области пользования личными устройствами фактически не контролируется. Что говорить, если даже бывшая госсекретарь США **Хиллари Клинтон** отправляла электронные письма, содержащие секретную информацию, с личного почтового ящика.

Разберем наиболее типичные угрозы и меры предосторожности при пользовании личными гаджетами.

Осторожно — шпион

— Возможности шпионских программ практически безграничны, так как таковы возможности устройств, на которых они устанавливаются. Приложение-шпион может использовать динамик и осуществлять фоновую прослушку, получить доступ к камере и записывать фото и видео происходящего вокруг, передавать геолокацию, контакты, переписки и переговоры, файлы и прочее, — говорит Парфентьев.

Вредоносная программа может попасть на устройство, если злоумышленник получит физический доступ к гаджету. Учитывая быстродействие процессоров современных устройств, на установку шпионских программ нужны считаные секунды. Но человек может и сам установить программу-шпиона на смартфон или компьютер, приняв ее за безобидное приложение или любой полезный софт. «Даже официальные магазины приложений AppStore и GooglePlay не проверяют исходный код программы, в которую могут быть «зашиты» шпионские возможности. Косвенно об этом могут говорить лишние разрешения, которые хочет получить программа. Хрестоматийный пример — «фонарик», которому для чего-то нужен доступ к вашей адресной книге, фотогалерее, геолокации. Но в случае с приложением такси, например, такие запросы вас уже не смутят, а сервис может и использовать разрешение по прямому назначению (определять местоположение), и шпионить заодно, — комментирует Парфентьев. — Узнать, стоит ли на смартфоне шпионское ПО, довольно сложно. Совет следить за тем, как быстро садится аккумулятор, бессмысленный — на уровень заряда влияет с десяток разных факторов». «Неспециалисту определить, что его устройство заражено шпионским ПО, практически невозможно, — подтверждает **В. В. Чебышев**, антивирусный эксперт «Лаборатории Касперского», — ведь одной из особенностей таких программ является скрытность — они должны оставаться незамеченными в системе ровно столько, сколько потребуется злоумышленникам. Наверное, единственный реалистичный способ определить, что на устройстве человека установлен такой зловред, — установить антивирусное решение».

Технические же меры предосторожности — это регулярно обновлять уже установленные приложения (разработчики закрывают обнаруженные уязвимости, и эти «заплатки» нужно загрузить), не отключать антивирусную программу на смартфоне и обновлять саму ОС. «Также имеет смысл регулярно проверять, какие приложения работают в фоновом режиме и получают лишний доступ (последние версии операционной системы Android позволяют в принудительном порядке отозвать фоновый доступ). Например, с приложением Uber возник скандал, когда оказалось, что даже при выключенной геолокации сервис получает информацию о местоположении пользователя. Но это только один из примеров — так работает множество других программ и умных устройств. Части из них для работы действительно нужно получать информацию в фоновом режиме. Например, умным станциям — они должны постоянно быть наготове ответить на запрос, поэтому «слушают» все, что происходит вокруг. Проблема в том, что информация для обработки уходит на серверы сервиса и мы не можем знать о том, кто имеет к ней доступ и насколько она защищена», — добавляет Парфентьев.

К слову, специалисты «СерчИнформ» отмечают, что совет вынимать аккумулятор из телефона на совещаниях или важных переговорах, чтобы избежать отслеживания, был актуален для более ранних моделей телефонов (когда контроль велся не на уровне шпионского ПО, а на уровне GSM-сот). Архитектура современных смартфонов очень близка к архитектуре компьютера — при отсутствии питания операционная система не запущена, а следовательно, не запущены и шпионские программы. Поэтому на конфиденциальных переговорах достаточно просто выключить устройство.

Личная беспечность

Впрочем, гораздо проще стать жертвой не большого технического заговора, а собственной халатности. Так, обычно все правила безопасности запрещают выходить на значимые ре-

peshkov © 123RF.com

COVID-19 на службе мошенников

По данным зарубежных исследований, при организации компьютерных атак в 98% случаев используют методы социальной инженерии. Атаки, основанные на методах социальной инженерии, сегодня имеют две отличительные особенности. Первая — эксплуатация темы пандемии. Это может быть спам-рассылка с вредоносным вложением или ссылкой на вредоносную программу/сайт. Отправители таких писем мимикрируют под известные организации (например, Всемирную организацию здравоохранения), предложения по установке шпионских приложений (например, карты распространения коронавируса), шокирующие фейковые новости или новости, эксплуатирующие наиболее актуальные вопросы (QR-коды на перемещения и т. п.).

Вторая особенность заключается в том, что в семейном режиме самоизоляции стационарный компьютер или ноутбук может использоваться по графику разными поколениями с присущими им особенностями. Допустим, госслужащий на рабочей «удаленке», сотрудник компании, закрытой на период пандемии, а также студенты, школьники или пенсионеры. То есть метод, который не сработал на одном члене семьи, прекрасно сработает на другом.

сурсы (корпоративные сервисы, почту) через браузеры, используя публичные точки доступа в интернет (открытые Wi-Fi-сети). Однако браузерный трафик очень легко перехватить. При необходимости решения рабочих вопросов со смартфона лучше воспользоваться сетью мобильного телефона, а не подключением общедоступной Wi-Fi-сети.

Мессенджеры, использующие так называемое сквозное шифрование (Telegram, WhatsApp, Viber и т. п.), — один из немногих вариантов вести относительно безопасные переписки и обмениваться файлами. «Разработчики мессенджеров постоянно работают над улучшением своих продуктов, в том числе с точки зрения безопасности. Например, внедряют сквозное шифрование, призванное сделать все сообщения и данные, которыми обмениваются собеседники, доступными только им. Однако нет таких переписок, к которым потенциально не могли бы получить доступ киберпреступники, если бы захотели. В прошлом году мы обнаружили новую версию шпионского зловреда FinSpy, которая может собирать данные в том числе и из тех мессенджеров, которые используют шифрование, таких как Telegram, WhatsApp, Signal и Threema. Иными словами, если телефон заражен подобным ПО и злоумышленники получат привилегированный доступ, то на таком устройстве они потенциально могут получить доступ к внутреннему хранилищу и истории переписок или же следить за общением пользователей буквально в режиме реального времени, внедрившись в процессы мессенджера», — комментирует Чебышев.

Настоятельно рекомендуется ограничить использование разного рода публичных сервисов, если речь идет о работе. Они не приспособлены для хранения и передачи конфиденциальной информации и документов. Пользовательские соглашения, которые никто не читает, не скрывают, что данные передаются третьим лицам для целей более точной настройки рекламы — это плата за бесплатность.

— Для многих стало откровением, что информация из закрытых сервисов время от времени оказывается в публичном доступе из-за неверных настроек конфиденциальности. Так, настоящим шоком оказалась история, когда в поиске «Яндекса» оказались загруженные в GoogleDocs документы. То же регулярно происходит с документами из сервиса для совместной работы Trello. ИБ-эксперты находили так секретные документы ООН и других общественных и государственных организаций. Пользователи забывали сменить настройку «доступно всему интернету», и документы индексировались для всеобщего обозрения, — говорит Парфентьев.

Возвращаясь к вопросу обеспечения цифровой безопасности высших должностных лиц: дилемма обычно заключается в том, что служба безопасности могла бы вовремя пресечь опасность, но она не имеет доступа к ПК и прочим устройствам руководителей. Поскольку они имеют доступ к конфиденциальной информации, которую специалистам по информационной безопасности знать не положено. «Все логично, но проблема решается очень просто. Например, у нас в компании реализовано два контура безопасности: один для рядовых сотрудников, второй — для топ-менеджмента. Ко второму контуру имеют доступ только два доверенных лица», — отметили в «СерчИнформ».

Т. С. МАКУРОВА