Это странное слово – BYOD. Странное, если не сказать больше…

Аббревиатура BYOD расшифровывается в виде английской фразы «Bring Your Own Device», переводится как «принеси собственное устройство» и означает активное использование в работе личных устройств. Примером такого использования может служить не только доступ с личного смартфона к рабочей электронной почте, но и использование бизнес-приложений (электронный документооборот, бухгалтерские и финансовые учётные системы, системы планирования снабжения и т.д.) на собственных планшетах сотрудников.

Среди несомненных преимуществ концепции называются следующие:

- Повышение производительности сотрудников, в том числе, за счёт увеличения мобильности сотрудников и использования личных устройств для работы во внерабочее время;
- Повышение удовлетворённости сотрудников от работы и большее удобство при работе благодаря возможности выбирать для работы адаптированное под персональные нужды, практически «родное», личное устройство;
- Сокращение затрат работодателя на оснащение рабочих мест и обеспечение рабочего процесса (ввиду того, что существенная часть затрат фактически переносится на сотрудников).

Оставляя за рамками данной короткой статьи степень «маркетинговости» данных утверждений, давайте посмотрим, какие следствия имеет внедрение данной концепции с точки зрения обеспечения информационной безопасности.

Проведённое в 2014 исследование компании «Лаборатория Касперского» показало, что 62% владельцев и сотрудников компаний в той или иной мере используют для работы личные мобильные устройства вне зависимости от размера компании. При этом 92% респондентов хранят важные корпоративные данные на смартфонах и планшетах, которые они используют как для работы, так и в личных целях. Из них 38% признали, что хранят на своих устройствах рабочие данные, которым определённо не следует попадать «не в те руки». По разным оценкам, около 85% мобильных устройств в мире работают под управлением операционной системы Android. Для которой в 2012 году было написано 99% вредоносных программ и вирусов, созданных для мобильных устройств (35000 новых вредоносных программ под Android было зарегистрировано только за 2012, что в 6 раз больше, чем в 2011).

Таким образом, несмотря на все преимущества концепции BYOD, в случае её внедрения, на работодателя неизбежно ложится серьёзная работа по «обороне» корпоративных данных (в том числе и прежде всего, конфиденциальных и персональных) от значительно возросшего количества потенциальных точек проникновения в корпоративную ИТ-инфраструктуру. В виде, будем откровенны, намного хуже, в отличие от корпоративных устройств, защищаемых личных мобильных устройств сотрудников.

Ведь в лучшем случае на личных устройствах используется лишь один «эшелон обороны» от всего широкого арсенала средств злоумышленников – устанавливается пароль на вход в устройство. Регулярно обновляемый антивирус на смартфоне или планшете и включённые функции удалённой блокировки устройства и удаления данных с устройства (в случае его утери или кражи) – всё ещё редкость. И уж совсем уникальная вещь – шифрование данных на устройстве с использованием более-менее надёжного алгоритма шифрования. А между тем всё это - абсолютно необходимые меры безопасности при использовании личных устройств для работы с корпоративными данными и системами!

Наиболее важным следствием для любого сотрудника при использовании им в работе личного устройства является тот факт, что его **личное устройство перестаёт быть личным**. В силу того, что компании необходимо защищать свои данные на личном устройстве сотрудника, у неё появляются основания для контроля состояния и работы личных устройств сотрудников. Это может выражаться в принятии специальной обязательной к исполнению политики использования личных мобильных устройств, регламентирующей порядок и способы использования устройств, содержащей, например, требования предоставления доступа к данным, хранимым на устройстве, ИТ/ИБ-службам компании, перечень разрешённого ПО и иные подобные положения, часто существенно ограничительного характера. Учитывая то, что на личных устройствах хранятся также личные (и даже очень личные!) данные, возникает довольно сложно решаемая дилемма: **как обеспечить безопасность корпоративных данных, не вторгаясь в**

личную жизнь сотрудников?

Разные компании решают эту дилемму диаметрально различными методами. Некоторые строго запрещают хранение корпоративных данных на личных устройствах и помещают корпоративные данные в закрытый сегмент ИТ-инфраструктуры, доступ в который со своих мобильных устройств имеют лишь «избранные». Другие официально объявляют личные устройства, используемые для работы, чуть ли не собственностью работодателя, а потому предполагается, что ИТ/ИБ-службы имеют полное право на любые манипуляции с личными устройствами сотрудников (включая установку ПО для удалённого и безвозвратного удаления всех данных на устройстве в случае его утери или кражи). При таком подходе личные устройства вполне могут стать средством слежения за сотрудниками со стороны работодателя.

Поэтому, совмещая «рабочее» и «личное», любому из нас всегда необходимо принимать во внимание те разносторонние следствия, которые это влечёт, учитывая баланс интересов работодателя и сотрудника. С одной стороны - удобство работы и свобода выбора «орудия труда». С другой – ответственное отношение к информационным активам компании, необходимость правильного и своевременного использования средств защиты информации и неотвратимая потребность «делиться» своим личным устройством с работодателем.

Подготовлено по материалам СМИ