

Издание: Ведомости
Автор: Николай Федотов
Город: Москва
Дата публикации: 27 марта 2008 г.



Опасный WiFi

Личные данные клиентов и финансовые показатели конкурентов не обязательно покупать на черном рынке или у специалистов по конкурентной разведке. Иные компании, увлекшись модными технологиями, сами открывают доступ к своим секретам

Ринат Сагдиев
Ведомости

Неделю назад Роман Ромачев, гендиректор компании «Р-техно», коротая время в ожидании автомобиля, обслуживаемого в «Тойота центр Измайлово», воспользовался гостевым компьютером, который салон предлагал клиентам. Профессиональный экономический разведчик, Ромачев решил проверить устройство внутренней компьютерной сети компании. Выйдя в интернет через точку беспроводного доступа WiFi, он, к своему удивлению, увидел в сетевом окружении 109 компьютеров центра, включая машины отдела маркетинга, приемки и бухгалтерии. Лишь некоторые компьютеры были защищены паролем, но даже начинающий хакер знает, как легко ломается доступ к ним через сеть, рассказал Ромачев «Ведомостям». «На гостевом компьютере можно было оставить вирус, который выкачивал бы нужные файлы из сети. Взломав компьютер с бухгалтерской программой “1С”, можно внести изменение в финансовую информацию или передать всю информацию конкурентам», — перечисляет потенциальные опасности Ромачев. Учитывая, что клиентам автосервиса предоставлен бесплатный доступ в интернет, все интересные файлы можно спокойно отправить себе на почту, продолжает он.

«Угроза проникновения в сеть действительно была», — признает сотрудник IT-службы сервисного центра. Гостевой компьютер был установлен год назад, для того чтобы клиентам, отдавшим автомобили на техобслуживание, было чем заняться, и лишь вчера, после обращения «Ведомостей», компания создала для него отдельную сеть, закрыв доступ к корпоративной информации.

Устанавливая в своих помещениях WiFi-доступ, компании часто забывают защитить себя, говорят эксперты. Сотрудник службы безопасности одной из российских госкорпораций вспоминает, как летом прошлого года просканировал карманным компьютером WiFi-сеть в аэропорту «Домодедово» и увидел информацию с нескольких компьютеров, принадлежащих, по

его предположению, туристическим агентствам. Там в свободном доступе лежали десятки отсканированных паспортов граждан Великобритании и Эфиопии, различные служебные письма турфирм с персональными данными клиентов, рассказал он «Ведомостям».

«Налицо несоблюдение обязанностей по защите персональной информации», — резюмирует Ромачев. На территории «Домодедово» развернуто несколько WiFi-сетей — не только общедоступная коммерческая сеть и служебная сеть аэропорта, но и сети авиакомпаний, турагентств и других арендаторов комплекса, объясняет начальник группы по работе со СМИ «Домодедово» Эльдар Тузмухаметов. «Мы защищаем только свою служебную сеть», — отмечает он.

При использовании беспроводных компьютерных технологий число открытых для публичного доступа компьютеров значительно увеличивается, предупреждает Максим Эмм, директор департамента аудита компании «Информзащита». Компании, привыкшие защищать от внешнего проникновения проводные компьютерные сети, забывают, что один гостевой компьютер, подключенный к WiFi, резко повышает риск утечки информации. Защита при этом очень проста: достаточно зашифровать беспроводной доступ к сети и установить сетевые экраны (программы, запрещающие несанкционированный доступ к компьютеру).

* * *

Кто ошибается

Около 1% беспроводных компьютерных корпоративных сетей открыто для публичного доступа из-за ошибок администраторов, подсчитал **главный аналитик агентства InfoWatch Николай Федотов**. Несколько процентов «дыр» на совести сотрудников компаний, несанкционированно установивших точки доступа WiFi. Более 90% сетей защищено по всем правилам, но и им не стоит расслабляться. По словам Федотова, большинство компаний используют для защиты беспроводных WiFi-сетей протокол безопасности WEP (Wired Equivalent Privacy), который был взломан хакерами несколько лет назад.

<http://www.vedomosti.ru/newspaper/article.shtml?2008/03/27/144434>