Опубликовано на Швейцария: новости на русском языке (https://nashagazeta.ch)

Дистанционная работа и кибербезопасность | Télétravail et cybersécurité

Автор: Лейла Бабаева, Женева-Лозанна-Цуг , 23.10.2020.

© nashagazeta.ch

При работе из дома киберриски намного выше, чем в офисе. Чего следует опасаться, какие меры нужно принять и как компании могут защитить сотрудников?

|

Avec le travail à distance, les cyberrisques sont plus grands que dans les bureaux de l’entreprise. A quoi faut-il penser, quelles mesure doit-on prendre et comment les compagnies peuvent-elles protéger leurs employés?

Télétravail et cybersécurité

Из-за пандемии все больше сотрудников разных компаний переходят на дистанционный режим работы. Можно подумать, что единственное изменение в этом случае – количество встреч с коллегами, но одновременно растет угроза кибератак, поскольку меняется оборудование, каналы связи, особенности работы с данными и круг лиц, которые имеют к ним доступ. Цифровые преступления опаснее обычных правонарушений, так как их часто констатируют спустя несколько месяцев после их совершения. Более того, во многих случаях о том, что кто-то проник в информационную систему, первой узнает не сама компания, а ее клиенты или партнеры, которые начинают жаловаться на проблемы, пишет газета Le Temps.

За примерами далеко ходить не нужно: в начале октября этого года Фрибургский университет сообщил, что в августе хакеры получили доступ к учетным записям и банковским данным семи сотрудников. В сентябре часовой гигант Swatch заявил, что стал жертвой масштабной атаки. Недавно Наша Газета рассказывала о том, что хакеры украли зарплаты преподавателей нескольких швейцарских вузов.

Задачу киберпреступникам облегчает то, что удаленным сотрудникам предоставляется постоянный доступ к информационной системе фирмы. Сегодня хакеры имеют больше лазеек, позволяющих им реализовать задуманное, так как домашние wi-fi-сети порой никак не защищены, при этом многие работают на личных компьютерах, не устанавливая на них пароли.

Пираты часто совершают атаки на самих пользователей, применяя методы фишинга, отправляя электронные письма со ссылками на сайты с компьютерными вирусами, прибегая к социотехнике, т.е. тактике проникновения, при которой взломщик обманным путем (например, представляясь новым сотрудником) получает важную информацию о компании или ее компьютерных системах. В итоге предприятие несет финансовые убытки, плюс приходится успокаивать взволнованных клиентов, объясняя им возможные последствия кражи их данных. Одно из лучших решений перед тем, как перевести работников на удаленное сотрудничество, – провести ликбез по компьютерной безопасности. Например, при работе за ноутбуком из кафе не следует ни на секунду оставлять устройство без присмотра, зато следует блокировать экран, если нужно позвонить по телефону или хочется отвлечься и спокойно допить кофе.

Со своей стороны, телекоммуникационные компании предлагают клиентам средства защиты. Специалисты Swisscom разработали разные решения, основанные на использовании информационных сетей, центров данных, облачных вычислений и средств обнаружения информационных угроз. Женевская фирма Infomaniak, предоставляющая услуги хостинга, заранее включила кибербезопасность во все свои предложения. Как только эксперты замечают подозрительную деятельность в учетной записи одного из клиентов, они сразу меняют пароль доступа и звонят клиенту, чтобы дать советы, как защитить себя от подобных проникновений.

Эксперты отмечают, что для обеспечения безопасности не обязательно покупать специальные программы. Последние могут гарантировать базовую защиту, но многое зависит от пользователя, и его беспечность может дорого ему обойтись. Не следует заходить на подозрительные сайты, нужно регулярно устанавливать обновления программ, делать резервные копии важных файлов и почаще менять пароли. Более того, необходимо использовать только рабочую электронную почту: это поможет сразу обнаружить злоумышленника, если он попытается участвовать в переписке с вашими коллегами, зарегистрировав почтовый ящик на постороннем сайте.

А как быть, если удаленный сотрудник живет в другой стране? Это актуально для Швейцарии, так как в числе работников местных компаний много фронтальеров. К счастью, киберриски для них не выше, чем для остальных, при условии использования VPN-сервисов (от английского Virtual Private Network – виртуальная частная сеть). Кроме того, будет полезно исключить возможность подключения к наиболее важным корпоративным ресурсам из внешней сети без VPN. Еще один нюанс – отключать VPN сразу же, как только вы закончили просматривать нужную базу данных или закрыли конкретную программу. Продуктивной вам работы!

Женева
кибербезопасность
кибербезопасность
Статьи по теме
Бум киберпреступности в Швейцарии
В кантоне Во киберпираты опустошают банковские счета
В Швейцарии будет развиваться киберспорт
В Швейцарии воруют в киберпространстве
Швейцария задолжала хакерам
У швейцарских преподавателей украли зарплаты

Source URL:
https://www.nashagazeta.ch/news/la-vie-en-suisse/distancionnaya-rabota-i-kiberbezopasnost