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

Готова ли Швейцария к кибервойне? | La Suisse est-elle préparée à la cyberguerre?

Автор: Заррина Салимова, Берн , 15.03.2022.

Фото: Clint Patterson, Unsplash

По оценкам экспертов, сайты швейцарских органов власти и финансовых учреждений могут стать мишенью хакеров, «мстящих» за введеные Федеральным советом санкции. Обычным интернет-пользователям также не стоит терять бдительность, чтобы не попасться на удочку интернет-мошенников.

|

Les experts estiment que les sites web des autorités et des institutions financières suisses pourraient être visés par hackers se «vengeant» des sanctions imposées par le Conseil fédéral. Les internautes ne doivent pas non plus baisser la garde, au risque d'être la proie de fraudeurs.

La Suisse est-elle préparée à la cyberguerre?

Санкции, которые Федеральный совет принял в отношении России, не остались без ответа. Прежде всего, Швейцария вместе с другими странами, которые ввели подобные ограничения, включая государства-члены Евросоюза, США и Великобританию, попала в российский список «недружественных стран». На практике это будет означать, что кредиторам из этих стран российские граждане и компании будут выплачивать долги в рублях. Но речь может идти не только об экономических последствиях – некоторые эксперты опасаются начала всеобщей кибервойны в Европе.

Первые «звоночки» уже были. Как сообщает RTS, 24 февраля, в день нападения России на Украину, тысячи модемов европейских частных лиц и компаний внезапно перестали работать. Модемы были подключены к Интернету через спутник KA-SAT, принадлежащий американской компании ViaSat, сигнал которого, по данным ряда СМИ, использовался также техникой украинской армии. Не исключено, что речь идет не о простом совпадении, а о целенаправленной хакерской атаке.

В электронном письме, направленном телеканалу RTS, Национальный центр кибербезопасности (NSCS) признал, что в качестве реакции на санкции следует ожидать, что сайты швейцарских органов власти и финансовых учреждений станут мишенью хакеров. Причем особенно осторожными должны быть компании, имеющие деловые отношения с поставщиками или фирмами, расположенными в зонах конфликтов.

Достаточно ли хорошо защищена Швейцария от кибератак? Банки, поставщики электроэнергии и атомные электростанции заверили журналистов RTS, что готовы к кибервойне. Так, Федеральная инспекция по ядерной безопасности (IFSN), выполняющая функции надзора за надежностью работы ядерных объектов в Швейцарии, сообщила, что швейцарские атомные электростанции в настоящее время не сталкиваются со значительным ростом кибератак в связи с войной в Украине. Меры ИТ-безопасности на АЭС выходят далеко за рамки обычных и строго контролируются, при этом особенно хорошо защищена ядерная часть объектов. Национальная компания, отвечающая за подачу электроэнергии, Swissgrid не раскрыла подробностей своей стратегии кибербезопасности, однако заявила, что осознает свою роль оператора критической инфраструктуры в Швейцарии и принимает все необходимые меры для обеспечения безопасности систем. Что касается альянса промышленных предприятий и региональных компаний по управлению энергией Swisspower, то он три года назад создал совместный центр кибербезопасности, который представляет собой группу реагирования на киберугрозы, специально направленные на энергетический сектор. Стоит отметить, что в июне 2021 года поставщики электроэнергии получили менее одного из четырех баллов за уровень «кибер-зрелости» в отчете, подготовленном по заказу федерального управления энергетики, но с тех пор представители отрасли усовершествовали систему безопасности. Наконец, Швейцарская ассоциация банкиров (ASB) сообщила, что швейцарские банки всегда применяли самые высокие стандарты безопасности и делают все возможное для предотвращения киберрисков.

Мишенью теоретически могут стать и телекоммуникации, в частности, подводные кабели, которые соединяют Европу с Интернетом. Как уточняет RTS, через этот маршрут проходит более 90% международного интернет-потока, причем примерно с 2014 года российские корабли неоднократно были замечены вблизи этой кабельной сети. В случае российской атаки Европа может остаться без международных телефонных звонков и Интернета, а также потерять доступ к сайтам, расположенным на зарубежных серверах. В пользу этой теории, по мнению экспертов, говорят и попытки России изолировать себя от глобальной интернет-сети путем создания собственной.

Добавим, что жертвами интернет-мошенников в эти неспокойные времена могут стать не только компании, но и обычные пользователи. Национальный центр кибербезопасности предупреждает, что злоумышленники пользуются текущей ситуацией для массовой рассылки мошеннических электронных писем с призывом сделать пожертвования – эксперты напоминают, что переводить средства стоит только проверенным организациям. Более того, некоторые швейцарские пользователи сообщили о получении писем якобы от ООН с предложением помочь жертвам войны в Украине, вложив в «инвестиционный проект» 500 евро и через неделю получив 8000 евро. Недоумение вызывает не только возможность заработать такую сумму за столь короткое время, но и то, почему обещанная прибыль должна пойти получателю письма, а не беженцам. Еще один пример мошенничества: некоторые электронные письма рассылаются якобы от имени украинского военно-морского инженера, который хотел бы вывезти из страны свою семью и состояние в один миллион франков и просит получателя письма помочь ему в этом. Взамен «инженер» предлагает передать часть своего состояния, правда, сначала ему нужно срочно перевести определенную сумму – это классическое мошенничество с авансовыми платежами. Национальный центр кибербезопасности также напоминает: если вы получили подозрительное письмо, не открывайте вложения и не переходите по ссылкам, так как вы можете заразить свой компьютер вредоносным программным обеспечением.

Швейцария
кибербезопасность
